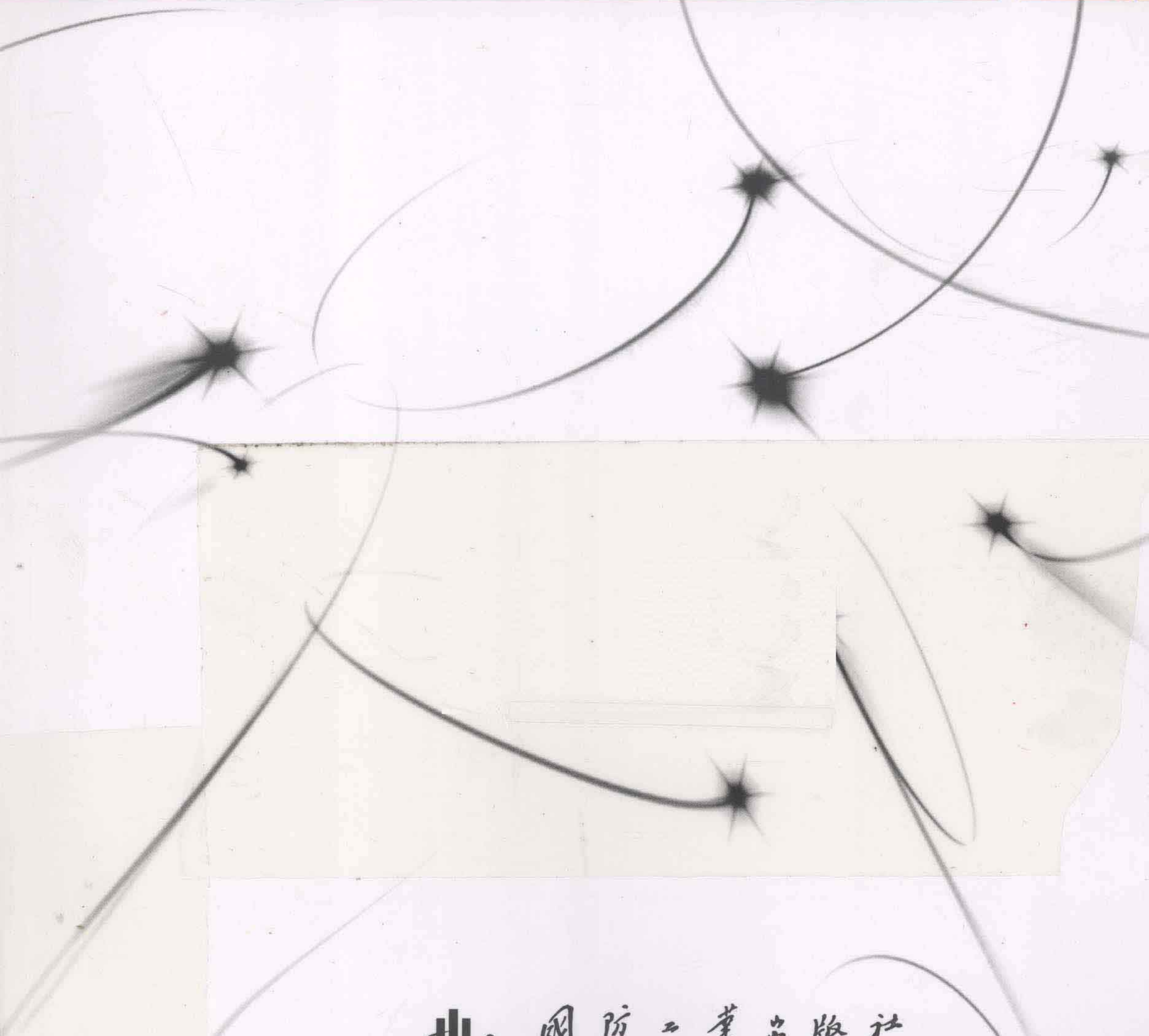
智能网络传感器与无线传感器网络

景博 张劼 孙勇 著



国防工业出版社
National Defense Industry Press

智能网络传感器与无线传感器网络

责任编辑：崔晓莉　xlcui@ndip.cn
责任校对：李莲凤
封面设计：陆　阳

▶ 上架建议：电工电子 ◀
http://www.ndip.cn
ISBN 978-7-118-06878-8
9 787118 068788 >
定价：68.00 元

智能网络传感器与无线传感器网络

景博 张劼 孙勇 著

国防工业出版社
·北京·

内 容 简 介

本书全面、系统地介绍了网络传感器与无线传感器网络，包括：基于以太网的智能网络传感器系统、无线智能网络传感器、无线传感器网络拓扑结构、组网协议，应用支撑关键技术，原型系统与应用实例。

本书内容丰富、条理清晰。既注重对基础知识的介绍，又紧密结合领域现状与发展趋势的讲解。

本书可用作计算机、电子和通信类专业本科生和研究生教材，也可供相关教学、科研和工程技术人员阅读和参考。

图书在版编目(CIP)数据

智能网络传感器与无线传感器网络 / 景博，张劼，孙勇著. —北京：国防工业出版社，2011.1

ISBN 978-7-118-06878-8

Ⅰ.①智… Ⅱ.①景… ②张… ③孙… Ⅲ.①智能控制-传感器 ②无线电通信-传感器 Ⅳ.①TP212

中国版本图书馆 CIP 数据核字(2010)第 252957 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 印张 27 字数 615 千字

2011 年 1 月第 1 版第 1 次印刷 印数 1—4000 册 定价 68.00 元

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

序

互联网和大规模移动通信技术的出现改变了人类的生产和生活方式,对经济社会的发展起到了巨大推动作用。进入21世纪以来,人类对物理世界即时感知的需求也越来越强烈。无线传感器网络作为传感技术、计算机技术、网络技术和通信技术交叉与融合的产物,它将地域上分散的、具有通信能力的传感器节点有机互联起来,为实现全球物理感知提供了可能,并在工业安全、交通管控、精细农业、环境监测、智能家居、远程医疗以及国防等领域都有广阔的应用前景。当前,世界不少发达国家都加大了对无线传感器网络研究的投入,力图占据领先位置。

本书从智能网络传感器和无线传感器网络的角度,分别讲解了网络化传感器和传感器网络化两大问题。事实上,网络化传感器早已有之,符合各种工业总线标准的智能化、网络化传感器已经得到广泛应用,但大规模传感器的组网问题无论从技术难度还是应用前景来看都很值得去研究、去探索。本书对无线传感器网络的基础理论、关键技术和国内外研究现状做了较为清晰和详实的论述。

无线传感器网络这一新兴产业的出现,为我国产业结构调整和优化提供了机遇。我国已将这项技术发展列入国家中长期科技发展规划,以抢占战略性新兴产业发展制高点。温总理深刻指出,“必须依靠科技创新和提高人才素质,培育新的增长点,在经济发展和科技创新上占领制高点,这样才能保证国家可持续发展能力和竞争力。”希望该书的出版能够为发展具有我国特色的传感器网络产业和培养信息科技人才发挥积极作用。

适逢出版之际,谨为之序。

张钟华

2010年1月20日

前　言

信息科学是众多学科中发展较快的一门科学,也是最具发展活力的学科之一。21世纪是人类全面进入信息电子化的时代,随着探索领域和空间的不断拓展,人们不再满足于多个传感器独立地对环境进行感知,而是希望通过大量传感器之间的相互协作实现更为广泛与精细的监测任务,同时将监测结果通过网络传送给相应的用户,以使用户完成更为复杂的计算、分析和处理。在此需求之下,无线传感器网络应运而生,成为当前国际上备受关注的热点研究领域。

传感器网络的发展大致经历了4个阶段。第一代传感器网络是由传统传感器组成的点到点信号传输的测控系统,采用二线制4mA~20mA电流或1V~5V电压实现传感器信号传输。这种系统曾经一度在测控领域广为应用,但由于其布线复杂、成本昂贵,抗干扰性差,已逐渐淡出市场。第二代传感器网络则是由智能传感器和现场控制器组成的测控系统,采用数字信号实现传感器信号传输,如RS-232、RS-485、RS-429等数字通信标准。这种系统是微处理器与传感器的发展相结合的产物,传感器具有了计算能力,可有效消除传统的通信方式所带来的传感器发展瓶颈。第三代传感器网络是基于现场总线的智能传感器网络,采用全数字、开放式的双向通信,可实现与互联网的连接。现场总线技术利用数字通信代替了传统的模拟信号,大大减少了传感器与主控系统的连线以及通信带宽,有效降低了系统成本与复杂度,特有的分层体系结构实现了分布式智能。

第四代传感器网络就是目前被广泛研究的无线传感器网络,它集成了嵌入式计算技术、微型传感器技术、无线网络技术、MEMS技术和低功耗电路技术等,通过各类集成化的微型传感器协作地实时监测、感知和采集各种环境或监测对象的信息,利用嵌入式系统对信息进行处理,并通过自组织无线通信网络以多跳方式将所感知信息传送到用户终端,从而真正实现"无处不在"的计算理念。无线传感节点之间利用无线链路取代电缆收发数据,这就克服了前三代传感器网络的诸多缺点。

无线传感网络在新一代网络中具有关键性,甚至决定性的角色,作为一种新的计算模式,推动科技发展和社会进步,已成为国际竞争的焦点和制高点。在国家安全、航空航天、环境监测、医疗救护、制造业和反恐抗灾等领域,特别是在未来军事领域中将掀起一股产业浪潮,引起一场划时代的军事技术革命和未来战争的变革。我国十分重视无线传感器网络的研究及其产业化,《中国未来20年技术预见研究》提出的157个技术课题中有7项直接涉及无线传感器网络。2006年初发布的《国家中长期科学和技术发展规划纲要(2006—2020)》为信息技术确定了3个前沿方向,其中,"传感器网络与智能信息处理"和"自组织网络技术"两个方向与无线传感器网络研究直接相关。

从无线传感器网络研究现状来看,未来的智能传感器网络难以被某一种架构所统治,

但会受应用需求的驱使而不断发展。可以说,无线传感器网络将是对21世纪产生巨大影响力的重要技术。

本书分为5篇,共18章。第1篇为智能网络传感器技术概述,分别介绍了基于以太网、无线网两种智能传感器系统。第2篇讲述了无线传感器网络体系结构与拓扑结构,分析了体系结构、网络拓扑结构及控制与网络部署、连通与覆盖等问题。第3篇集中介绍了无线传感器网络的通信协议,重点介绍了无线传感器网络物理层协议、MAC协议和路由协议。第4篇主要阐述了应用支撑与关键技术,包括时钟同步、节点定位、网络接入技术、服务质量保障与网络安全与可靠性等问题,尤其对Sink节点接入以太网传输协议进行了研究。第5篇给出了无线传感器网络系统平台及开发实例,描述了当前无线传感器网络的应用范例和原型验证系统,特别提出了无线传感器网络模拟器的设计,并介绍了无线传感器网络硬件平台开发和设计的基本方法,最后列出了国内外有影响的实例。

在本书部分资料收集、图表制作、文字校对过程中还包含了杨洲、周宇、郝中波、姜兴旺、程帅的辛勤劳动,在此表示衷心感谢。撰写和出版过程中得到了国防工业出版社和空军工程大学领导的大力支持,正是你们的辛勤工作,才使得本书如期付梓。

本书编写过程中参考了大量文献和资料,互联网是其中一个重要来源,在此对原作者深表谢意。书中内容如有涉及相关人士的知识产权,请给予谅解并及时与我们联系。感谢您对本书内容提出批评和修改建议,我们将不胜感激。

作 者

2010年1月于西安

目 录

第1篇 智能网络传感器技术

第4篇 无线传感器应用支撑与关键技术

第5篇 无线传感器原型系统与应用实例

第1篇

智能网络传感器技术

第1章　智能网络传感器系统

传感器技术、通信技术与计算机技术构成现代信息技术的三大基础，它们分别完成对被测量的信息感知、信息传输及信息处理，是当代科学发展的重要标志。随着科学技术的发展，数字化、智能化和网络化已成为时代发展趋势：计算机技术和通信技术结合产生了计算机网络技术；计算机技术和传感器技术结合产生了智能传感器技术；将两者融为一体，即计算机网络技术与智能传感器技术结合，便产生了智能网络传感技术。智能网络传感器是以嵌入式微处理器为核心，集成了传感单元、信号处理单元和网络接口单元，使传感器具备自检、自校、自诊断及网络通信功能，从而实现信息的采集、处理和传输真正统一协调的新型智能传感器。它使传感器不再仅仅是采集与处理器件，而是集采集、处理与通信于一体的智能体。

网络化智能传感技术实现了传感器的网络化和智能化，从根本上改变了信息获取能力和信息控制能力。从空间域上讲，将会大大突破人类获取信息的地理空间限制，实现真正意义上的大规模信息获取与控制；从时域上讲，各种"即插即用(Plug & Play)"传感器的应用将会大大缩短传感器应用和配置的时间。这种新的信息获取能力和控制能力将会大大提高工业生产效率，改变工业、农业、军事、医疗、教育等诸多领域的现状。

1.1　传感器技术发展概述

传感器是工业应用的灵魂，是人类探知自然界信息的触角，它可将人们需要探知的各种非电量信息转化成可测的电量信息，是信息系统的第一道门槛，为人们认识和控制相应的对象提供条件和依据。作为现代信息技术3大核心技术之一的传感器技术，从诞生至今，已经经历了"聋哑传感器"(Dumb Sensor)→"智能传感器"(Smart Sensor)→"智能网络传感器"(Networked Sensor)的发展历程。

1. 聋哑传感器

这种传统的传感器是模拟仪器仪表或模拟计算机时代的产物，其设计指导思想是把外部信息变换成模拟电压或电流信号，输出幅值小、灵敏度低，且功能单一，因而被称为聋哑传感器。

2. 智能传感器

随着时代的进步，传统的传感器已经不能满足现代工农业生产甚至战争的需求，20世纪70年代以来，计算机技术、微电子技术、光电子技术获得迅猛发展，加工工艺逐步成熟，新型敏感材料不断出现，在高新技术的渗透下，尤其是计算机硬件和软件技术的渗入，人们把微处理器和传感器相结合，开发了具备一定数据处理能力，并能自检、自校、自补偿的新一代传感器——"智能传感器"。智能传感器的出现是传感技术的一次革命，对传感

器的发展产生了深远影响。

3. 智能网络传感器

20 世纪 80 年代以来，网络通信技术逐步走向成熟并渗透到各行各业，各种高可靠、低功耗、低成本、微体积的网络接口芯片被开发出来，微电子机械加工技术（MEMS）的飞速发展给现代加工工艺注入了新的活力，人们把网络接口芯片与智能传感器集成起来并把通信协议固化到智能传感器的 ROM 中，导致了网络传感器的产生。网络传感器继承了智能传感器的全部功能，并且能够和计算机网络进行通信，如在现场总线控制系统中得到了广泛应用，成为现场级的数字化传感器。此外，人工智能、专家系统、模糊理论、神经网络等也加强了对传感技术的影响，增强了传感器的“智能化”功能。

1.2　智能网络传感器概述

1.2.1　智能网络传感器概念与原理

智能传感器是通过在普通传感器内部嵌入微处理芯片，具有将模拟信号转换成数字信号、加工处理原始感知数据等功能，并能通过标准接口与外界进行数据交换的一种传感器。智能传感器的原理结构如图 1.1 所示。

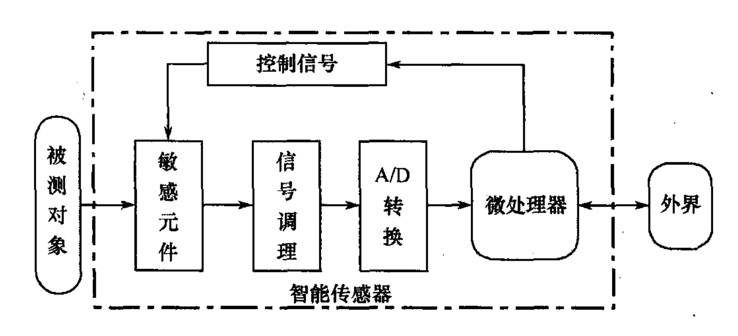


图 1.1　智能传感器原理结构图

敏感元件从被测对象得到模拟信号，经信号调理和 A/D 转换后送到微处理器进行数据处理，之后通过接口传送到外界。相反，外界也可将测试命令信号送到微处理器中，通过微处理器向敏感元件发送测试指令，进行数据采集。与传统的聋哑传感器相比，智能传感器具有以下优点：

（1）具有逻辑思维与判断、信息处理功能，可对感知数据进行分析、修正和误差补偿，提高了测量精度。

（2）具有自诊断、自校准功能，提高了可靠性。

（3）具有组态功能，可实现多传感器、多参数复合测量，扩大了检测与使用范围。

（4）具有存储功能，可随时存取检测数据。

（5）具有数据通信功能，能与计算机直接联机，相互交换信息，实现对传感器的初始化、校正和配置等操作。

随着计算机技术、网络技术和通信技术的迅速发展，智能传感器也顺应这一发展趋势，在新需求的推动下，逐步与网络相结合，出现了网络化的智能传感器——智能网络传

感器。网络化使智能传感器又增加了许多新功能,具有了许多新优势。

智能网络传感器遵从某种网络通信协议,在测试现场将测得数据发送到网络上,使其能够在一定范围内实时发布和共享。智能网络传感器原理结构如图 1.2 所示。

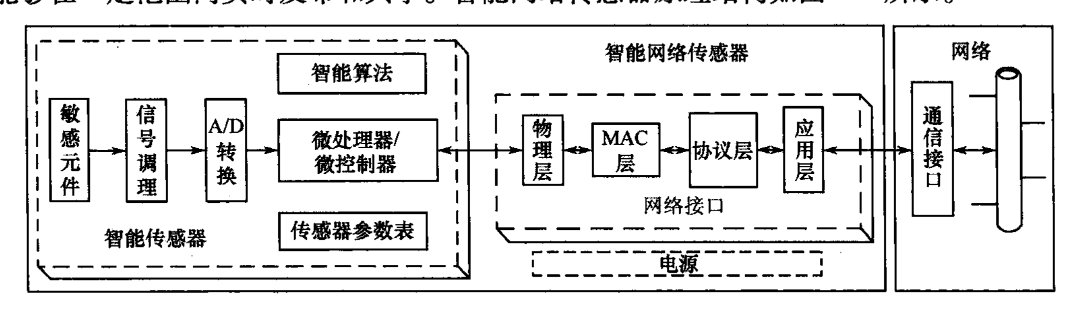


图 1.2　智能网络传感器原理结构图

智能传感器输出的数字信号,由网络处理装置根据通信协议加以封装并附上地址,然后通过网络接口发送上网。反过来,网络处理装置又能接收网络上其他节点的数据和命令,并将其传送给智能传感器,从而实现对它的操作和控制。由此看来,网络化智能传感器是测试网络中一个独立的节点,能够独立地完成测试任务,是实现网络化测试的基础。

智能网络传感器的核心是嵌入式微处理器。嵌入式微处理器具有微体积、微功耗、可靠性高、可抗干扰能力强等特点。带有高速 CMOS Flash/EEPROM,片内可以集成多个通道的 A/D 转换模块。可以实现模拟量与数字量之间的转换,完成信号数据的采集、处理(如数字滤波、非线性补偿、零点漂移与温度补偿、自诊断与自保护等)和数据输出调度(包括数据通信和控制量本地输出)。因此,传感器的线性度和测量精度大大提高。同时,由于传感器已进行了大量的信息预处理,不但减少了测控系统中主控站的负担,而且减少了系统的信息传输量,可以使系统的可靠性和实时性大大提高。

智能网络传感器使传感器由单一功能、单点检测向多功能和多点检测发展;从被动检测向主动进行信息处理方向发展;从现场测量向远程实时在线测控发展。网络化使得传感器可以就近接入网络,传感器与测控设备间再无需点对点连接,大大简化了连接线路,节省成本,易于系统维护,也使系统更易于扩展与升级。

智能网络传感器研究的关键技术之一是网络接口技术。智能网络传感器必须符合某种网络协议,使现场测控数据能直接进入网络。由于目前工业现场存在多种网络标准,因此也随之发展起来了多种智能网络传感器,具有各自不同的网络接口单元类型。网络的选择可以是传感器总线、现场总线,也可以是企业内部的以太网(Ethernet),也可以直接是因特网(Internet)。目前,主要有基于现场总线和基于以太网协议的两大类智能网络传感器。根据应用需求和系统现场运行的实际情况,可以采用有线智能网络传感器或无线智能网络传感器。无线智能网络传感器的数据传输可利用电磁波、红外线等无线传播介质,电磁波具有很强的抗干扰、抗噪声和抗衰减能力,使用的频段主要是工业科学医疗频段(Industrial Scientific and Medical,ISM),如 433MHz、915 MHz 和 2.4GHz 等,不会对人体造成伤害,而红外线适合开阔无障碍的应用环境。

1.2.2　智能网络传感器实现途径

智能网络传感器的实现通常有非集成化、集成化和混合实现 3 种方式。

非集成化智能网络传感器是将经典传感器（采用非集成化工艺制作的传感器，仅具有获取信号的功能）、信号调理电路、带数字总线接口的微处理器及网络接口组合为一整体而构成的一个智能网络传感器系统，其框图如图 1.3 所示。

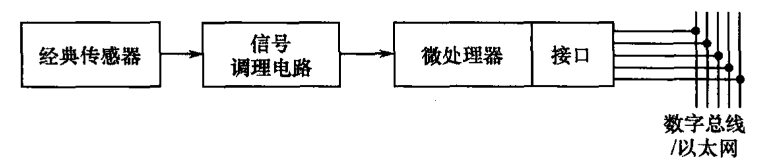


图 1.3　非集成式智能网络传感器框图

图 1.3 中的信号调理电路用来调理传感器输出的信号，即将传感器输出信号进行放大并转换为数字信号后送入微处理器，再由微处理器通过数字接口接入现场数字总线或以太网上。这是一种实现智能网络传感器系统的最快途径与方式，这种非集成化智能网络传感器是在现场总线控制系统发展形势的推动下迅速发展起来的。对于自动化仪表生产厂家来说，原有的一整套生产工艺设备基本不变，而需要挂接一定数量的智能传感器/变送器，又不希望对现有传感器作较大的改动。因此，对于这些厂家而言非集成化实现是一种建立智能网络传感器系统最经济、最快捷的方式。

集成化智能网络传感器（Integrated Intelligent Networked Sensor）系统是采用微机械加工技术和大规模集成电路工艺技术，利用硅作为基本材料制作敏感元件、信号调理电路、微处理器单元、网络接口电路（网络接口可分离），并把它们集成在一块芯片上而构成的。这种智能网络传感器具有如下特点：

（1）微型化。例如，微型压力传感器可以装在飞机或发动机叶片表面用以测量气体的流速和压力。美国最近研究成功的微型加速度计可以使火箭或飞船的制导系统质量从几千克下降至几克。

（2）结构一体化①。采用微机械加工和集成化工艺，使硅杯一次整体成型，而且电阻变换器与硅杯是完全一体化的。进而可在硅杯非受力区制作调理电路、微处理器单元、网络接口电路，甚至是微执行器及网络接口，从而实现不同程度的，乃至整个系统的一体化。

（3）高精度。传感器结构一体化将使迟滞、重复性指标大为改善，精度得到有效提高。后续的信号调理电路与敏感元件一体化后可大大减小由引线长度带来的寄生参量的影响，这对电容式传感器更有特别重要的意义。

（4）多功能化。微/纳米级敏感元件结构的实现特别有利于在同一硅片上制作不同功能的多个智能网络传感器，如可同时集成感受压力、压差及温度参量的敏感元件，这样不仅增加了传感器的功能，而且可以通过数据融合技术消除交叉灵敏度的影响，提高传感器的稳定性与精度。

（5）阵列式。微/纳米技术已经可以在 $1cm^2$ 的硅芯片上制作成千上万个传感器。然而，要在一块芯片上实现智能传感器系统存在着许多困难和棘手的难题。例如，哪一种敏感元件比较容易采用标准的集成电路工艺来制作；选用何种信号调理电路，如精密电阻、电容、晶振等，不需要外接元件；由于直接转换型 A/D 变换器电路太复杂，制作了敏感元

① 压阻式压力传感器是最早实现一体化结构的智能型传感器。

件后留下的芯片面积有限,需要寻求其他 A/D 转换的形式;由于芯片面积有限制,以及制作敏感元件与数字电路的优化工艺的不兼容性,微处理器系统及可编程只读存储器的规模、复杂性与完善性受到很大限制;对功耗与自热、电磁耦合带来的相互影响,在一块芯片内如何消除等。

(6)全数字化。数字量的使用将为智能网络传感器提供极为稳定的性能,精度高、不需 A/D 转换器便能与微处理器方便地接口。对于节省芯片面积、简化集成工艺,均十分有利。

若按具有的智能化程度来分,集成化智能网络传感器有中级形式/自立形式和高级形式两种存在形式。

中级形式是以微处理器单元为核心,组成环节包括敏感单元、信号调理电路、网络接口电路,一个完整的传感器系统全部封装在一个外壳里的形式。它具有完善的智能化网络功能,这些智能化网络功能主要是由强大的软件(包括相关的通信协议)来实现的。

高级形式是集成度进一步提高,敏感单元实现多维阵列化时,同时配备了更强大的信息处理软件,具有更高级的智能化功能的形式,而且还具有更高级的传感器阵列信息融合功能,或具有成像与图像处理等功能。从而可有效提高网络通信部分的效率及实时性。对于集成化智能传感器系统而言,集成化程度越高,其智能化程度和网络使用效率也就越可能达到更高的水平。

由于在一块芯片上实现智能网络传感器,并不总是必需的,所以更实际的途径是混合实现。根据需要与成本,将系统各个集成化环节,如敏感单元、信号调理电路、微处理器单元、数字总线接口、网络接口以不同的组合方式集成在 2 块或 3 块芯片上,并装在一个外壳里。

1.2.3　有线智能网络传感器

目前,有线智能网络传感器主要有基于现场总线的网络化智能传感器和基于以太网的网络化智能传感器两大类。两种传感器技术比较起来,各有特点和适用范围,在应用上还存在着一定的互补性。

两种技术的基本思想都是针对传统测控系统的不足,使得检测信号在现场级就实现全数字化,从而避免了模拟信号在传输过程中信号易衰减和易受干扰等问题。因此,二者在底层的硬件部分结构大致相同。基于现场总线的网络化智能传感技术和基于以太网的网络智能传感技术的最大区别在于信号的传输方式和网络通信策略,也体现在后者独特的 TCP/IP (Transmission Control Protocol/Internet Protocol,传输控制协议/互联网协议)功能上。

1.2.3.1　基于现场总线的智能网络传感器技术

现场总线正是在现场仪表智能化和全数字控制系统的需求下产生的,是连接智能现场设备和自动化系统的数字式、双向传输、多分枝结构的通信网,其关键标志是支持全数字通信,主要特点是高可靠性。它可以把所有的现场设备(仪表、传感器与执行器)与控制器通过一根线缆相连,形成现场设备级、车间级的数字化通信网络,可完成现场状态监测、控制、远传等功能。传感器等仪表智能化的目标是信息处理的现场化,这也正是现场总线技术的目标,是现场总线不同于其他计算机通信技术的标志。

由于现场总线技术明显的优越性,在国际上已成为一个研究开发的热点。各大公司都开发出了自己的现场总线产品,形成了自己的标准。目前常见的标准有数十种,它们各

具特色,在各自不同的领域都得到了很好的应用。

基于现场总线技术的智能网络传感器目前还面临着诸多问题,主要原因正是多种现场总线标准的并存。例如,目前的智能网络传感器有基于基金会现场总线 FF 标准的,也有基于 ProfiBus 标准的,在我国对基于 RS－485 总线的网络传感器的研究则较多。由于现存的数十种现场总线标准互不兼容,不同厂家的智能传感器都采用各自的总线标准。因此,目前智能传感器和控制系统之间的通信还以模拟信号为主,或者是在模拟信号上叠加数字信号,这显然要大大降低通信速度,也严重影响了现场总线式智能传感器的应用。

为了解决这一问题,IEEE 和 NIST(National Institute of Standards and Technology)联合发起制订了一个简化控制网络和智能传感器连接标准,即灵巧传感器接口标准(Smart Sensor Interface standard)IEEE1451。标准采用通用的 A/D 或 D/A 转换装置作为传感器的 I/O 接口,将应用的各种传感器的模拟量转换成标准规定格式的数据,连同一个小存储器——传感器电子数据表 TEDS(Transducer Electronic Data Sheet)与标准规定的处理器目标模型——网络适配器 NCAP(Network Capable Application Process)连接,这样,数据可以按网络规定的协议接入网络。

该标准从面向对象的角度定义了网络化智能变送器的有关接口,可以把硬件和软件模块相结合以实现各类网络应用系统的功能。它为智能传感器和现有的各种现场总线提供了通用的接口标准,将有利于现场总线式智能网络传感器的发展与应用。表 1.1 列出了 IEEE1451 智能变送器标准体系各成员的名称、描述与当前状态,表中代号中的字母"P"(Proposed)表示该标准目前的状态是提议标准,还没有颁布和执行。

表 1.1　IEEE1451 智能变送器标准体系

代号	名称与描述	状态
IEEE P1451.0	智能变送器接口标准	待颁布
IEEE 1451.1－1999	网络适配器信息模型	颁布标准
IEEE 1451.1(修订)	网络适配器信息模型	修订中
IEEE 1451.2－1997	变送器与微处理器通信协议和 TEDS 格式	颁布标准
IEEE 1451.2(修订)	变送器与微处理器通信协议和 TEDS 格式	修订中
IEEE 1451.3－2003	分布式多点系统数字通信与 TEDS 格式	颁布标准
IEEE 1451.4－2004	混合模式通信协议与 TEDS 格式	颁布标准
IEEE P1451.5	无线通信协议与 TEDS 格式	待颁布
IEEE P1451.6	CANopen 协议变送器网络接口	开发中
IEEE P1451.7	USB	研讨中

图 1.4 描述了 IEEE1451 标准体系的整体框架和各成员间的关系(IEEE P1451.6 和 IEEE P1451.7 未在图中列出),其中,IEEE1451.x 虽然是互相协同工作的,但它们也可以彼此独立发挥作用。IEEE1451.1 可以不需要任何 IEEE1451.x 硬件接口而使用,IEEE1451.x 硬件接口也可以不需要 IEEE1451.1,但其软件必须提供相应的功能,如传感器数据或信息的网络传输。

1.2.3.2　基于以太网的智能网络传感技术

随着计算机网络技术的快速发展,将以太网直接引入测控现场成为一种新的趋势。

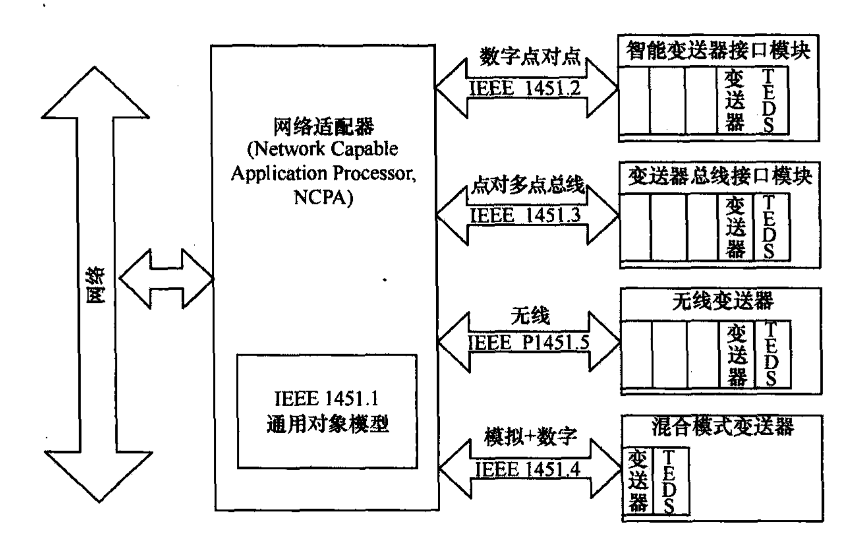


图 1.4　IEEE1451 智能传感器/执行器接口标准族体系结构

以太网技术由于其开放性好、通信速度高和价格低廉等优势已得到了广泛应用。人们开始研究基于以太网络即基于 TCP/IP 协议的网络化智能传感器。基于 TCP/IP 协议的智能传感器通过网络介质可以直接接入因特网或内联网(Intranet),还可以做到“即插即用”。在传感器中嵌入 TCP/IP 协议,使传感器具有因特网/内联网功能,相当于因特网上的一个节点。各种现场信号均可在网上实时发布和共享,任何网络授权用户均可通过浏览器进行实时浏览,并可在网络上的任意位置根据实际情况对传感器进行在线控制、编程和组态等。任何一个智能传感器可以就近接入网络,而信息可以在整个网络覆盖的范围内传输。

由于采用统一的网络协议,不同厂家的产品可以互换,互相兼容。但是,以太网直接应用于工业现场在技术上还受到一些限制,其主要缺点在于通信实时性差,网络安全性与可靠性低。与现场总线相比,还不能实现总线供电和远距离通信。通信的不确定性使其无法满足某些现场级的要求。

目前的趋势是将现场总线与以太网的融合,如 LXI(Lan eXtension for Instrumentation)总线。对于其他类总线,目前的主要做法是在各类总线的基础上,通过接口技术将智能传感器接入以太网,从而使现场总线技术具有采用标准以太网连线、使用标准以太网连接设备、采用 IEEE802.3 物理层和数据链路层网络协议标准及 TCP/IP 协议组等特点。总之,基于以太网的智能网络传感器仍有许多问题有待进一步研究。

1.2.4　无线智能网络传感器

在大多数测控环境下,传感器采用有线方式接入检测系统,而在无人区、偏远地区、战场等特殊的测控环境下使用有线电缆传输传感器信息是不方便的,不能够满足现实需要。随着无线技术的发展,无线接入方式在很多场合都得到应用以取代原有的有线接入方式。无线智能网络传感器势必成为传感器发展的一个重要方向,将使人们的生活成为真正的信息世界,给人们生活带来巨大的变化。无线传感器系统是新一代传感器系统,较有线传感器系统有如下优势:

(1)易于部署。传感器随机部署在感兴趣的地方而无需事先规划,降低安装成本和增加部署灵活性。

(2)范围扩展。许多分布的小型无线传感器覆盖的范围超过一个有线传感器的覆盖范围。

(3)容错能力。单个传感节点的故障不会影响网络的性能。

(4)移动性节点。可进行任意不脱离中心的移动。

为此,人们开发了多种无线通信方式的网络化智能传感器,目前比较常用的无线通信技术有蓝牙技术(Bluetooth,IEEE 802.15.1)、射频技术(RF)、超宽带无线技术(Ultra Wide Band)、ZigBee 技术(IEEE 802.15.4)等。下面重点介绍蓝牙技术、ZigBee 技术和 RF 技术。

1.2.4.1 蓝牙传感器系统

蓝牙技术是一种无线数据与语音通信开放性全球规范,是由 Ericsson、IBM、Intel、Nokia 和 Toshiba 等公司于 1998 年联合主推的一项最新的短距离无线通信技术,它是实现语音和数据无线传输的开放性规范,其实质是建立通用的无线空中接口及其控制软件的公开标准,使不同厂家生产的设备在没有电线或电缆相互连接的情况下,能在近距离(0.1m~100m)范围内使用,最大符号速率为 1Mb/s,将各种移动与固定通信设备、计算机及其终端设备等连接起来,具有互用、互操作的性能,在小范围内实现了无缝的资源共享。蓝牙设备工作在全球通用免申请的 2.4GHz ISM(Industrial、Scientific、Medical)频段,即工业、科学、医疗频段。无需许可证,给厂商生产、销售蓝牙设备以极大的便利条件。集成了蓝牙技术的设备体积小、功耗低、价格便宜,适合于工业设备的成本控制和运行开销,从而满足大量产品应用的需求,可广泛应用于工业现场、自动化控制等领域。

与传统的以电缆和红外方式传输测控数据相比,在测控领域应用蓝牙技术的主要优点如下:

(1)抗干扰能力强。采集测控现场数据经常遇到大量的电磁干扰,而蓝牙因采用了跳频扩频技术,故可以有效地提高数据传输的安全性和抗干扰能力。

(2)无需铺设电缆线,降低了环境改造成本,方便了数据采集人员的工作。

(3)没有方向上的限制,可以从各个角度进行测控数据的传输。

(4)可以实现多个测控仪器设备间的联网,便于进行集中测量与控制。蓝牙在测控系统的无线测量、监控、保护、自动控制以及生产线综合自动化测控和无线网络化测控系统等方面有着很强的应用能力,使测控系统移动数据交换、无线网络化、透明化和一体化成为可能,扩大和增强了测控系统的功能。

蓝牙技术还具有许多其他优点,如工作频段全球通用,使用方便、安全,抗干扰能力强,兼容性好、尺寸小,功耗低、多路多方向连接。

鉴于蓝牙技术的特点及优点,提出了一种蓝牙无线传感器来替代传统的传感器,从而构成蓝牙无线传感器控制系统,消除设备间繁琐的连线。蓝牙无线传感设备不同于传统电子设备间一对一的连接,而是一点对多点的连接。这种通过无线电波进行无线连接的方式可使多个智能的现场设备相互对话和互通信息,从而彻底消除了传统工业现场中难以理清的缆线,不同类型的接线板(它是信息传递技术中的致命弱点)也随之消失。

蓝牙无线传感器系统主要包括两大模块：传感器模块（Sensor Module）和蓝牙无线模块（Bluetooth Module）。前者主要用于进行现场信号的数据采集，将现场信号的模拟量转化为数字量，并完成数字量的变换和存储。后者运行蓝牙无线通信协议，使得传感器设备满足蓝牙无线通信协议规范，并将现场数据通过无线的方式传送到其他蓝牙设备中。两模块之间的任务调度、相互通信，以及同上位机通信的流程由控制程序控制完成。控制程序包含一种调度机制，并通过消息传递的方式完成模块间的数据传递以及同其他蓝牙设备的通信，从而完成整个蓝牙无线系统的功能。

蓝牙无线传感器硬件结构如图 1.5 所示。其中，基带单元（BB）和射频单元（RF）构成了蓝牙无线传感器的无线发射部件，负责执行信道分配、链路创建、控制数据分组等功能，并将数据转换成无线信号通过天线发射出去。

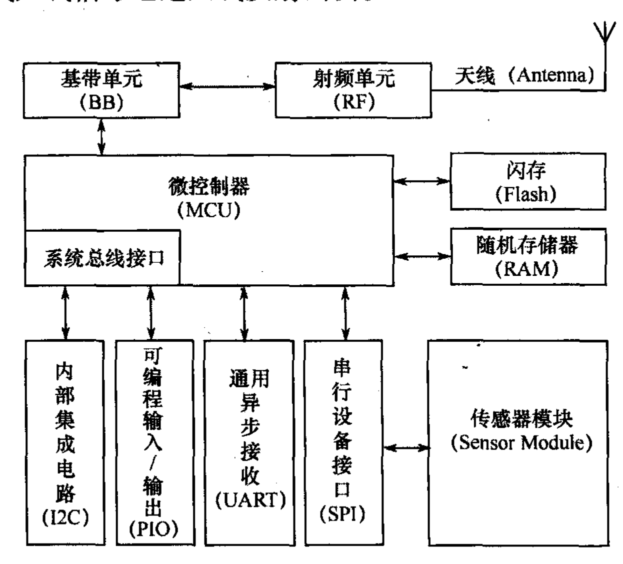


图 1.5　蓝牙无线传感器硬件结构图

传感器模块包括 A/D 转换、存储寄存器、通信 I/O 等部件，并通过标准内部集成电路总线接口（I^2C）与系统相连。现场数据的采集和无线通信由存储于闪存（Flash）的控制程序进行控制。当系统上电启动时，控制程序被调到随机存储器 RAM 中，在微控制器 MCU 的控制下运行。微控制器相当于计算机的中央处理器，连接系统的各个组成部分，完成系统的控制、运算、通信等功能，并负责执行系统的调度。

此外，蓝牙无线传感器还包括了一些外部通信接口组件，如串行设备接口（SPI）、可编程 I/O 接口（PIO）、通用异步收发接口（UART）、内部集成电路总线接口（I^2C）等。这些通信组件接口连接到微控制器（MCU）的系统总线接口，分别用于完成程序下载、状态指示、用户操作、程序调试，以及模块间通信等功能。

蓝牙无线传感器的内部软件结构如图 1.6 所示，最底层是应用程序接口（API），由相关的函数库、硬件接口程序组成，构成了整个系统软件框架的基础。应用程序接口（API）的上层是任务调度（TS）模块和蓝牙协议栈（BPS）。前者用于系统各任务的创建、执行和通信，后者执行蓝牙无线通信的底层协议。任务调度（TS）模块是用户应用程序（UI）的基础，而蓝牙协议栈（BPS）则保证了蓝牙无线传感器符合蓝牙无线通信规

范的要求。

蓝牙无线传感器可同任何其他符合蓝牙通信规范的蓝牙设备组成微网网络，在微网中蓝牙设备数量不超过 8 个，只有 1 个蓝牙设备是主设备，但是可以有 7 个从设备，连同上位机一起组成控制系统，进行现场信号的数据采集和设备监控。其网络结构如图 1.7 所示。

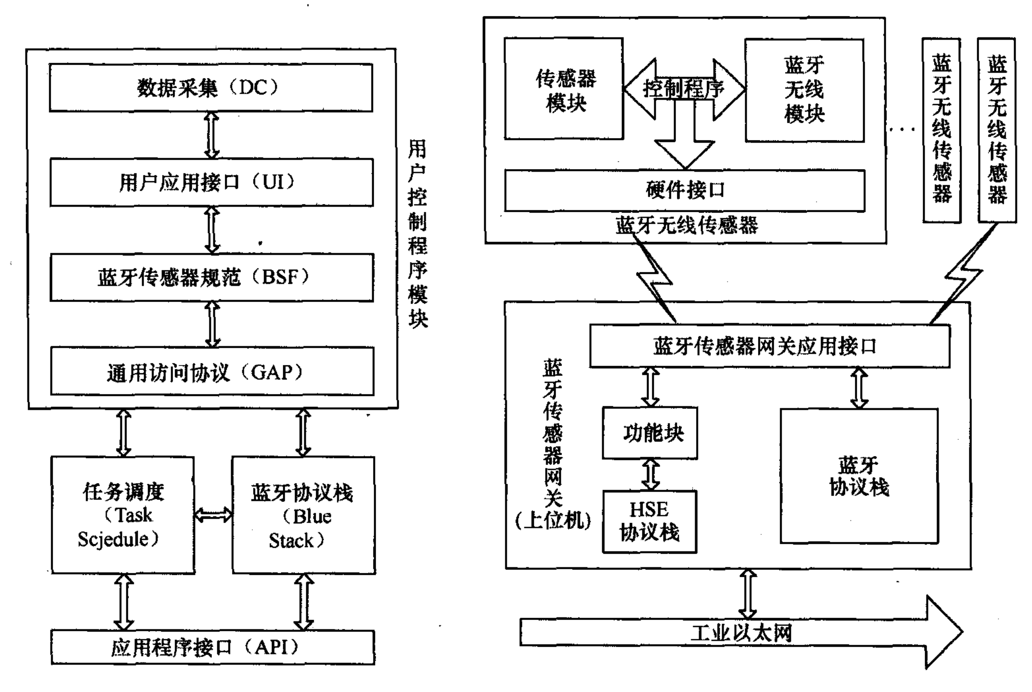


图 1.6　蓝牙无线传感器内部软件结构图

图 1.7　蓝牙无线传感器构成微网络结构图

将 IEEE 1451.2 标准和蓝牙技术结合起来设计无线智能网络传感器，以解决原有有线系统的局限。无线网络化传感器由 STIM、蓝牙模块和 NCAP 共 3 部分组成，在 STIM 和蓝牙模块之间是 IEEE1451.2 协议定义的 8 线 TII 接口。蓝牙模块通过 TII 接口与 STIM 相连，通过 NCAP 与因特网相连，承担了传感器信息和远程控制命令的发送和接收任务。NCAP 通过分配的 IP 地址与网络（内联网或因特网）相连。

无线网络化传感器与有线网络化传感器相比除增加了两个蓝牙模块外，其余部分一致。对于蓝牙模块部分，标准的蓝牙电路使用 RS－232 或 USB 接口，而 TII 是一个控制链接到它的 STIM 的串行接口。因此，必须设计一个类似于 TII 接口的蓝牙电路，构造一个专门的处理器来完成控制 STIM 和转换数据到用户控制接口 HCI（Host Control Interface）的功能。国外有不少公司已推出了基于蓝牙技术的硬件和软件的开发平台，如爱立信的蓝牙开发系统 EBDK、AD 公司的快速开发系统 QSDKe，利用开发系统可方便、快速地开发出基于蓝牙协议的无线发送和接收的模块。其体系结构如图 1.8 所示。

1.2.4.2　ZigBee 传感器系统

ZigBee 技术是一种新兴的短距离、低复杂度、低速率、低功耗、低成本的双向无线网络通信技术。ZigBee 技术并不是完全独有、全新的标准。它的物理层、MAC 层和链路层采用了 IEEE802.15.4（无线个人区域网）协议标准，相对 IEEE 1451.2 标准和蓝牙技术结合

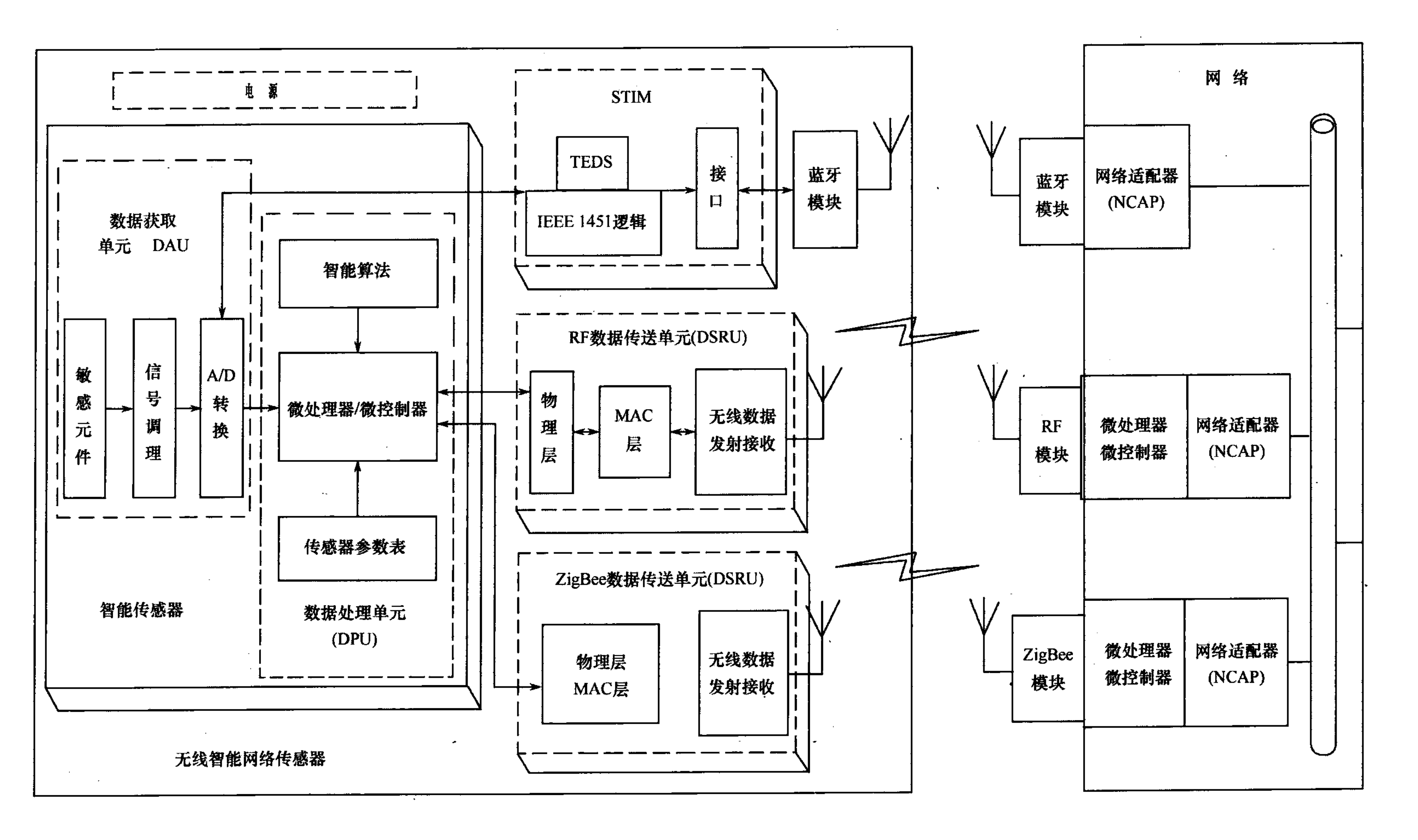


图 1.8 无线网络化传感器的体系结构

的方案,智能网络传感器无线化的设计与开发难度大大降低了。其网络层、应用会聚层和应用层规范(API)由 ZigBee 联盟制定,整个协议架构如图 1.9 所示。

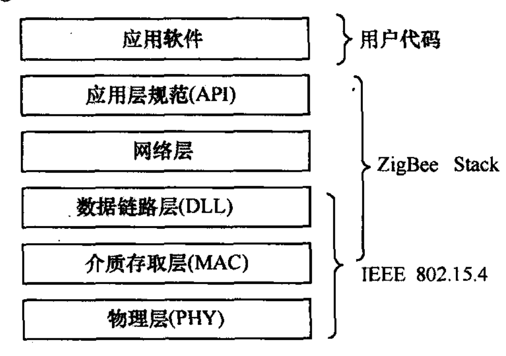


图 1.9　ZigBee 协议架构

ZigBee 依据 IEEE802.15.4 标准,可以在数以千计的微小的传感器之间实现通信,这些传感器以接力的方式通过无线电波将数据从一个传感器传到另一个传感器,所以它们的通信效率非常高。其主要技术特点包括低功耗、低成本、低速率、近距离、短时延、高安全和高容量。ZigBee 可采用星状、片状和网状网络结构,由一个主节点管理若干子节点,最多一个主节点可管理 254 个子节点,同时主节点还可由上一层网络节点管理,最多可组成 65 000 个节点的较大网络。利用 ZigBee 技术组成的 ZigBee 无线传感器系统结构简单、体积小、性价比高、放置灵活、扩展简便、成本低、功耗低、安全可靠,这种新兴的无线传感器系统必将有广泛的应用前景。

将 IEEE1451.5 标准和 ZigBee 协议相结合可以构建 ZigBee 无线传感器,该传感器系统由 STIM、TII 和 NCAP 三部分组成,基本结构如图 1.10 所示。

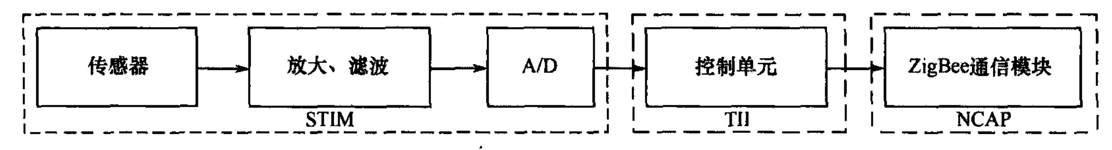


图 1.10　ZigBee 无线传感器系统基本结构图

STIM 部分包括传感器、放大滤波电路、A/D 转换;TII 部分主要由控制单元组成,控制单元负责链路管理与控制,执行基带通信协议和相关的处理过程,另外通过网络控制器连接各种网络;NCAP 主要是 ZigBee 通信模块,负责数据的无线收发,主要包括模拟接受器/模拟发射器和数字接受器两部分,前者提供数据通信的空中接口,后者主要提供链路的物理信道和数据分组。

基于 ZigBee 无线传感器可以实现 ZigBee 无线传感器网络,其基本结构如图 1.11 所示。此方案的实现,相当于在 IEEE1451.2 的结构模型上用无线接口取代了有线的 TII 接口,通过在 STIM 和 NCAP 中嵌入 ZigBee 模块,采用 ZigBee 协议实现了 STIM 和 NCAP 之间的无线数据传输。

1.2.4.3　普通 RF 射频无线通信

采用普通 RF 射频芯片构建无线通信模块,通信模块经无线接口接入智能传感器,并通过自定义物理层和 MAC 层协议标准,实现智能网络传感器无线化,这种方案是目前网络传感器无线化的一个主要手段。

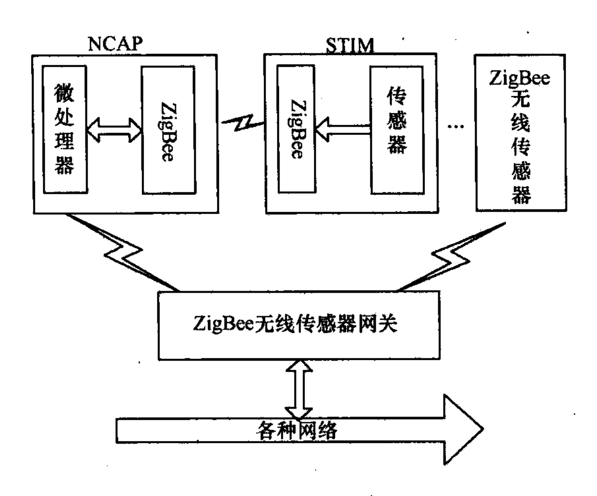


图 1.11　ZigBee 无线传感器网络基本结构图

1.3　智能网络传感器系统体系结构

要使智能网络传感器成为独立节点，具有网络节点的组态性和互操作性，实现就近接入网络，甚至实现"即插即用"，其关键是网络接口的标准化。下面分别介绍基于 IEEE1451.2 标准的智能网络传感器体系结构和基于 TCP/IP 的智能网络传感器体系结构。

1.3.1　基于 IEEE1451.2 标准的智能网络传感器体系结构

IEEE1451.2 是一种网络标准接口。IEEE1451.2 标准中仅定义了接口逻辑和 TEDS 的格式，其他部分由传感器制造商自主实现，以保持各自在性能、质量、特性与价格等方面的竞争力。同时，该标准提供了一个连接智能变送器接口模型 STIM(Smart Transducer Interface Module)和 NCAP 的 10 线的标准接口—变送器独立接口 TII(Transducer Independence Interface)，主要定义二者之间点点连线、同步时钟的短距离接口，使传感器制造商可以把一个传感器应用到多种网络和应用中。符合 IEEE1451 标准的有线智能网络传感器的典型体系结构如图 1.12 所示。

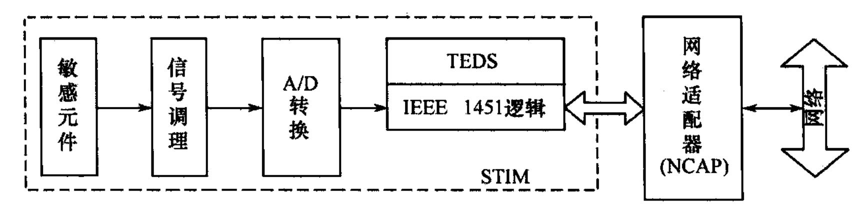


图 1.12　基于 IEEE1451 的智能网络传感器体系结构

其中，STIM 模块是连接变送器与 NCAP 模块的标准数字接口，主要提供了对变送器的访问、控制和数据的处理。模块主要包括变送器(传感器或执行器)，信号调理电路和 A/D、D/A 转换器，电子数据表单(TEDS)，接口电路(TII)，嵌入式微控制器和存储器。NCAP 用来连接 STIM 模块和网络，运行网络协议栈和应用固件。

当电源加上 STIM 时，变送器自身带有的内部信息，如制造商、数据代码、序列号、使用的极限、未定量以及校准系数，可以提供给 NCAP 及系统的其他部分。当 NCAP 读入一个 STIM 中 TEDS 数据时，NCAP 可以知道这个 STIM 的通信速度、通道数及每个通道上变送器的数据格式（12 位还是 16 位），并且知道所测量对象的物理单位，知道怎样将所得到的原始数据转换为国际标准单位。

在同 STIM 通信的过程中 NCAP 一直是主机，通信速率由 NCAP 设定，这会影响 STIM 中的采样速率，但是这避免了释放数据以及对存储器的巨大的需求。当 STIM 连接到 NCAP 时，NCAP 从 TEDS 读取有关 STIM 的信息，之后读取 STIM 采样的数据。变送器电子数据单 TEDS 分为可以寻址的 8 个单元部分，其中 2 个是必须具备的，其他的是可供选择的，主要为将来扩展所用。

基于 IEEE1451.2 标准和蓝牙协议的无线智能网络传感器由 STIM、蓝牙模块和 NCAP 三部分组成，其体系结构如图 1.13 所示。在 STIM 和蓝牙模块之间是 IEEE1451.2 协议定义的 10 线 TII 接口。蓝牙模块通过 TII 接口与 STIM 相连，通过 NCAP 与因特网相连，承担了传感器信息和远程控制命令的发送和接收任务。NCAP 通过分配的 IP 地址与网络（内联网或因特网）相连。

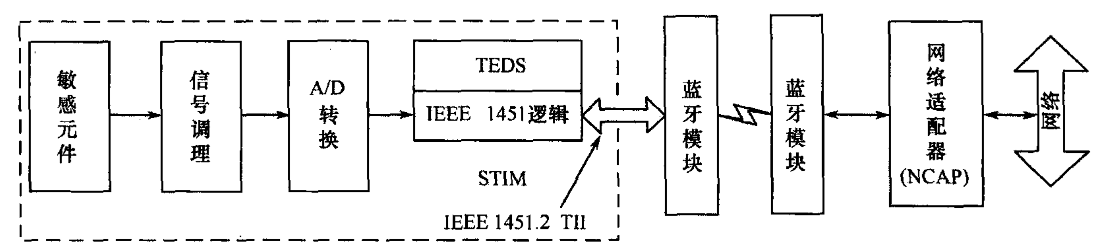


图 1.13　无线智能网络传感器体系结构

与基于 IEEE1451.2 标准有线智能网络传感器相比，上述无线智能网络传感器除增加了两个蓝牙模块外，其余部分相同。

1.3.2　基于 TCP/IP 协议的智能网络传感器体系结构

基于 TCP/IP 的智能网络传感器是把计算机网络的国际标准——TCP/IP 协议引入到了智能传感器中，即在传感器中嵌入了简化的 TCP/IP 协议，使传感器不通过 PC 或其他专用设备就能直接接入因特网/内联网。基于 TCP/IP 的智能网络传感器体系结构如图 1.14 所示。

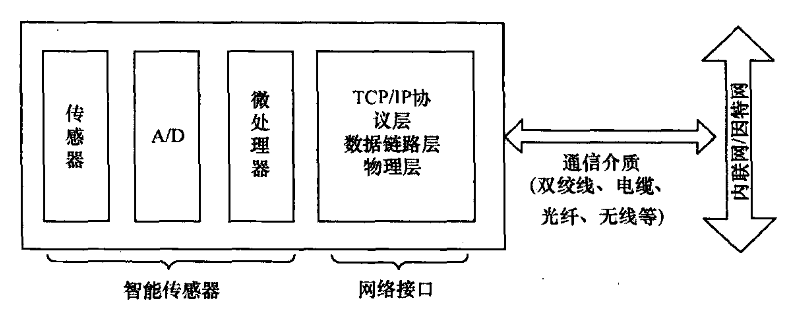


图 1.14　基于 TCP/IP 的智能网络传感器体系结构

基于 TCP/IP 的智能网络传感器把 TCP/IP 作为一种嵌入式应用，即把 TCP/IP 协议嵌入到智能传感器的 ROM 中，使得信号的收发都以 TCP/IP 方式进行，这样在传感器现场级就具备了 TCP/IP 功能，测控系统在数据采集、信息发布及系统集成等方面都以企业的内联网为依托，使得测控网和信息网统一起来。各种现场信号均可在企业的内联网上实时发布和共享，任何网络授权用户均可通过 IE 和 Netscape 浏览器实时浏览这些现场信息，为决策提供实时数据参考。如果企业内联网与因特网相连，各种现场信息均可在整个因特网上实时浏览，并可实现在整个因特网/内联网上任何位置对现场传感器的在线控制、编程和组态等，这为远程操作开辟了又一崭新道路。

基于 TCP/IP 的智能网络传感器实现了传感器的信息化，即实现因特网/内联网功能，具有划时代的进步意义，将对工业测控、智能建筑、远程医疗、环境和水文监测及农业科技应用等领域带来革命性的影响；它的另一重要意义是使测控系统本身发生了质的飞跃——在现场即可方便搭建基于内联网/因特网的测控系统。

在基于 IEEE1451.2 标准和基于 TCP/IP 协议的智能网络传感器基础上，可构建网络化测控系统。测控系统实现了网络化后，便能对大型复杂系统进行远程测控，对各种数据及相应的软件进行共享，这是信息时代的必然产物。利用智能网络传感器构建的网络化测控系统基本结构如图 1.15 所示。

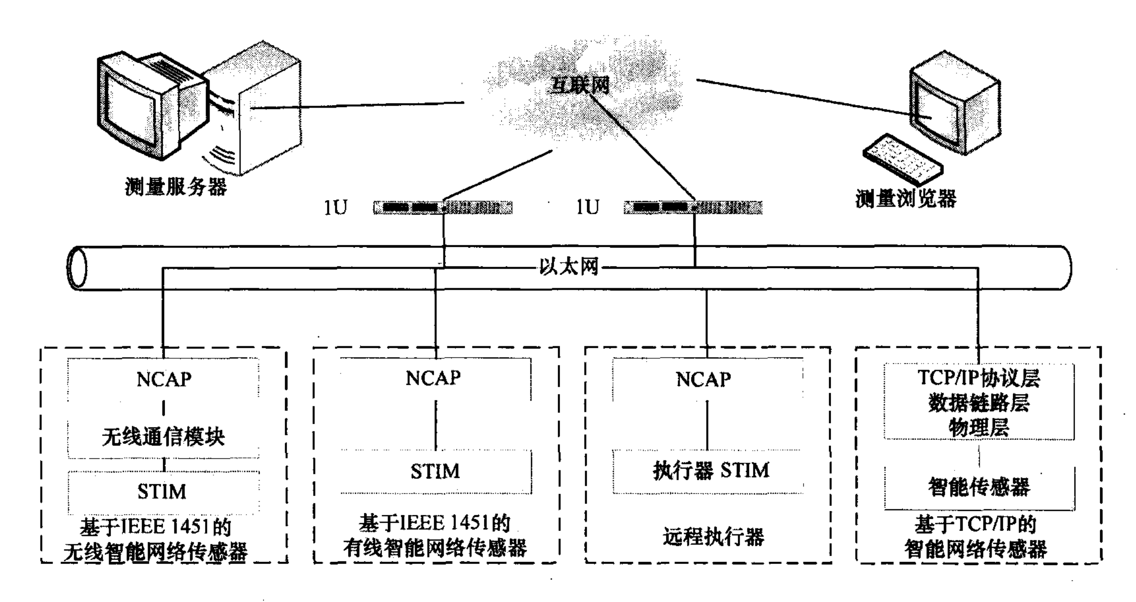


图 1.15　网络化测控系统基本结构

在图 1.15 所示的系统结构中，测量服务器主要对各种测量基本功能单元的任务分配，对基本功能单元采集来的数据进行计算、处理与综合，数据存储、打印等；测量浏览器为 Web 浏览器或别的软件接口，可以浏览现场测量节点测量、分析、处理的信息和测量服务器收集、产生的信息；智能网络传感器系统中，传感器不仅可以与测量服务器进行信息交换，而且符合 IEEE1451 标准的传感器、执行器之间也能相互进行信息交换，以减少网络中传输的信息量，也有利于系统实时性的提高。

1.4　智能网络传感器系统发展趋势

智能网络传感器系统的发展主要有以下 3 种趋势：

(1)传感器的敏感元件及其信号调理电路与微处理器和网络接口电路集成在一块芯片上的发展趋势。

(2)基于实际需求和经济性考虑，传感器(通过信号调理电路)与微处理器、微型计算机赋以智能化和网络化的结合，即智能网络传感器就是一种带有微处理器兼有检测信息、信息处理和信息网络化功能的传感器。这种模式突破了功能模块必须在工艺上集成在一块芯片上的框框，而是着重于微处理器、传感器和网络的智能结合。

(3)混合趋势，即以上两种方式的有机结合。

第2章　基于以太网的智能网络传感器系统

智能网络传感器的一个研究重点是传感器的网络化问题，要求智能传感器能直接和计算机网络进行数据通信、网络上的任何节点能对网络传感器进行数据访问、信息实时发布与共享以及对传感器在线编程和组态等。

智能网络传感器在构建网络时，能确定每个传感器的全局地址、组地址和设备识别号ID地址。用户通过网络就能获取任何一只传感器的数据，并对该传感器的参数进行设置。这样不仅提高了测量精度，还极大地方便了用户。此外，通过网络中各传感器之间、传感器与执行器之间、传感器与系统之间可实现数据交换及资源共享，在更换传感器时无需进行标定和校准，可做到“即插即用”。

2.1　基于以太网的智能网络传感器系统概述

在传统的网络通信中，大多数嵌入式设备仍处于孤立应用阶段，为了实现多个MCU之间的信息共享和交流，通常利用CAN、RS－232和RS－485等总线组成网络系统，以实现信息的交换，但存在传输距离短、容易受到外部干扰、可靠性差且孤立于因特网外等问题。随着计算机通信技术的发展，出现了智能网络传感器。

智能网络传感器是一个嵌入式系统，主要由3部分组成：敏感单元、智能处理单元和能够实现相关通信协议的网络接口，如图2.1所示。嵌入式智能网络传感器使传感器在现场级就实现了因特网/以太网/内联网功能，实现了测控网和信息网的统一。

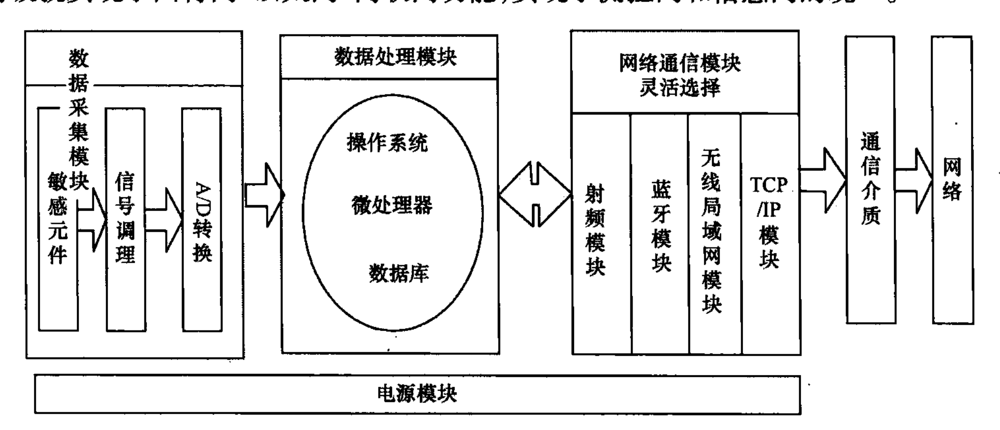


图2.1　嵌入式智能网络传感器一般结构

基于以太网的嵌入式智能网络传感器是在传统传感器的基础上嵌入了TCP/IP协议，采用以太网标准接口，主要由传感器单元、信号采集及处理单元、微处理器和以太网接口单元等部分组成，其结构如图2.2所示。

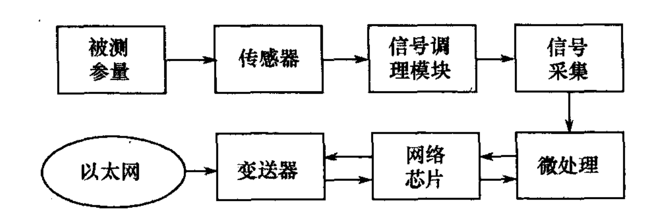


图 2.2 基于以太网的嵌入式智能网络传感器结构示意图

其工作原理是通过将被测参量转换为电信号,并经过电信号调理和 A/D 采集转换为数字信号,再经过微处理器的数据处理,包括零位漂移、温度漂移的补偿、滤波及校准后,由 TCP/IP 协议实现 TCP/IP 数据包的封装,最后通过以太网接口模块完成与计算机网络数据交换。

2.2 以太网协议标准与 TCP/IP 协议栈

2.2.1 工业以太网协议

由于商用计算机普遍采用的应用层协议不能适应工业过程控制领域中现场设备之间的以太网要求,所以必须在以太网和 TCP/IP 协议的基础上,建立完整有效的通信服务模型,制定有效的以太网服务机制,协调好工业现场控制系统中实时与非实时信息的传输,形成被广泛接受的应用层协议,也就是所谓的工业以太网协议。目前已经制定的工业以太网协议有 MODBUS/TCP、PROFInet、以太网/IP、HSE 等。

法国施奈德公司推出透明工厂的战略,使其成为工业以太网应用的坚决倡导者,该公司于 1999 年公布了 MODBUS/TCP 协议。MODBUS/TCP 协议以一种非常简单的方式将 MODBUS 帧嵌入 TCP 帧中。这是一种面向连接的方式,每一个呼叫都要求一个应答。这种呼叫/应答的机制与 MODBUS 的主从机制相互配合,使交换式以太网具有很高的确定性。利用 TCP/IP 协议,通过网页的形式可以使用户界面更加友好,并且利用网络浏览器就可以查看企业网内部的设备运行情况。施奈德公司已经为 MODBUS 注册了 502 端口,这样就可以将实时数据嵌入到网页中,通过在设备中嵌入 Web 服务器,就可以将 Web 浏览器作为设备的操作终端。MODBUS/TCP 协议框图如图 2.3 所示。

德国西门子公司于 2001 年发布其工业以太网的规范,称为 PROFInet,规范主要包括 3 个方面的内容。基于组件的对象模型(COM)的分布式自动化系统,规定了 PROFInet 现场总线和标准以太网之间开放透明通信;提供了一个独立于制造商,包括设备层和系统层的模型。PROFInet 的基础是组件技术,在 PROFInet 中,每一个设备都被看成是一个具有 COM 接口的自动化设备,同类设备都具有相同的 COM 接口。在系统中可以通过调用 COM 接口来调用设备功能。组件对象模型使不同制造商遵循同一个原则创建的组件之间可以混合使用,简化了编程。每一个智能设备都有一个标准组件,智能设备的功能通过对组件进行特定的编程来实现。同类设备具有相同的内置组件,对外提供相同的 COM 接口。为不同设备的厂家之间提供了良好的互换性和互操作性。图 2.4 是 PROFInet 的实时数据优化通信通道模型。

美国罗克韦尔公司于 2000 年分布工业以太网规范,称为 Ethernet/IP。Ethernet/IP 是

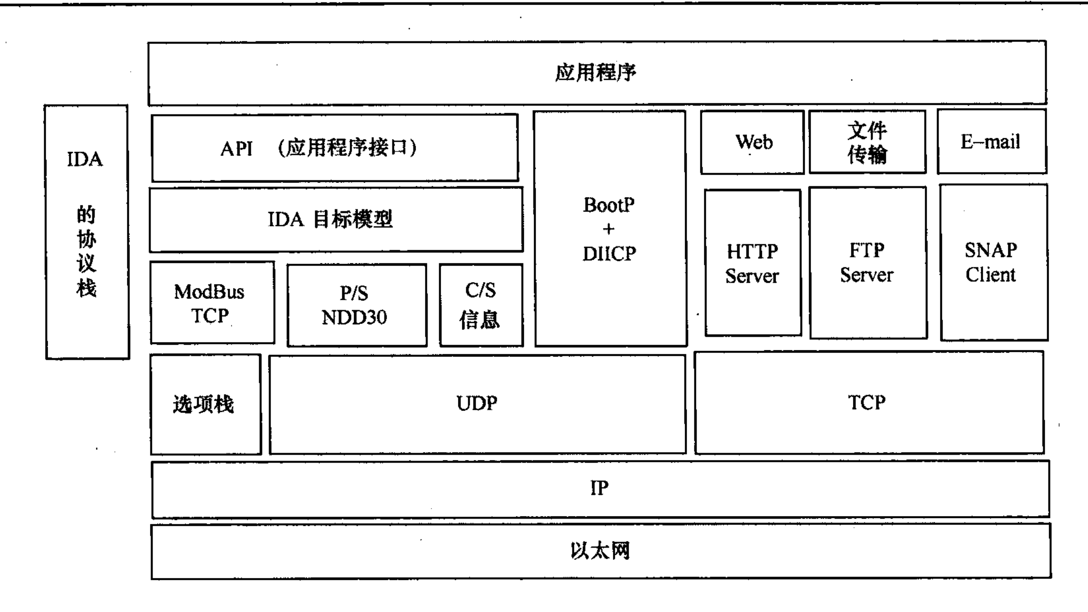


图 2.3　MODBUS/TCP 协议框图

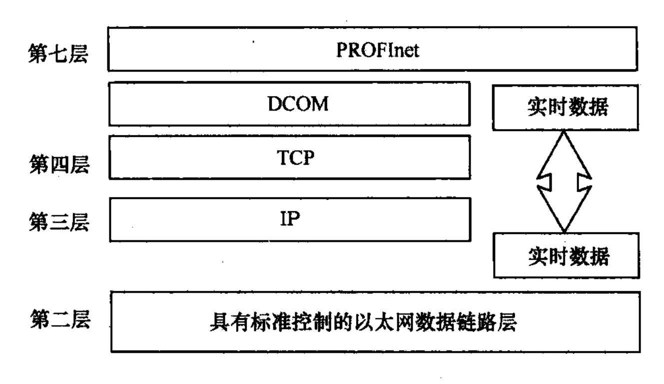


图 2.4　PROFInet 的实时数据优化通信通道模型

一种工业网络标准,它很好地采用了当前应用广泛的以太网通信芯片以及物理媒体。IP 代表 Industrial Protocol,以此来与普通的以太网进行区别。它是将传统的以太网应用于工业现场层的一种有效方法,允许工业现场设备交换实时性强的数据。Ethernet/IP 模型由 IEEE802.3 标准的物理层和数据链路层、以太网 TCP/IP 协议和控制与信息协议 CIP 三部分组成,其通信协议模型如图 2.5 所示。CIP 是一个端到端的面向对象并提供了工业设备和高级设备之间的连接的协议,CIP 有两个主要目的,一是传输同 I/O 设备相联系的面向控制的数据,二是传输同其他被控系统相关的信息,如组态、参数设置和诊断等。CIP 协议规范主要由对象模型、通用对象库、设备行规、电子数据表、信息管理等组成。

FF 现场总线基金会于 2000 年发布工业以太网规范,称为 HSE。HSE 是以太网协议 IEEE802.3、TCP/IP 协议族和 FF H1 的结合体。FF 现场总线基金会将 HSE 定位于实现控制网络与以太网的集成。由 HSE 连接设备将 H1 网段信息传输到以太网的主干网上,这些信息可以通过互联网送到主控室,并进一步送到企业的 ERP 和管理系统。操作员可以在主控室直接使用网络浏览器查看现场运行情况,现场设备也可以通过网络获得控制信息。

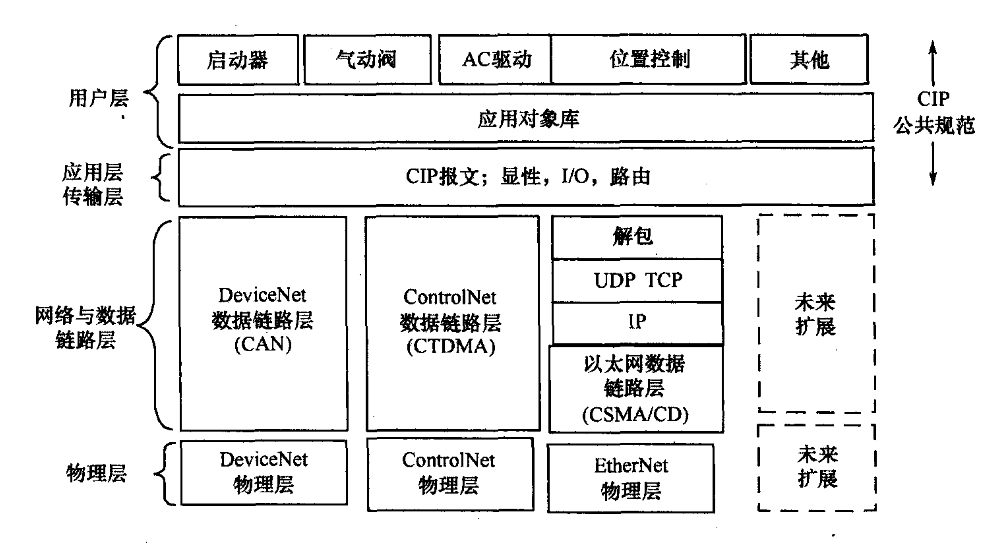


图2.5 InterNet/IP通信协议模型

HSE工业以太网为连续的过程控制工业和断续的制造业所需的连续实时控制提供了各种解决方案。它为连续过程控制系统、断续制造的控制系统、批量控制系统以及MES、ERP等企业信息管理系统的集成，提供了一种相当成熟的工业以太网标准协议。HSE的通信协议栈如图2.6所示。

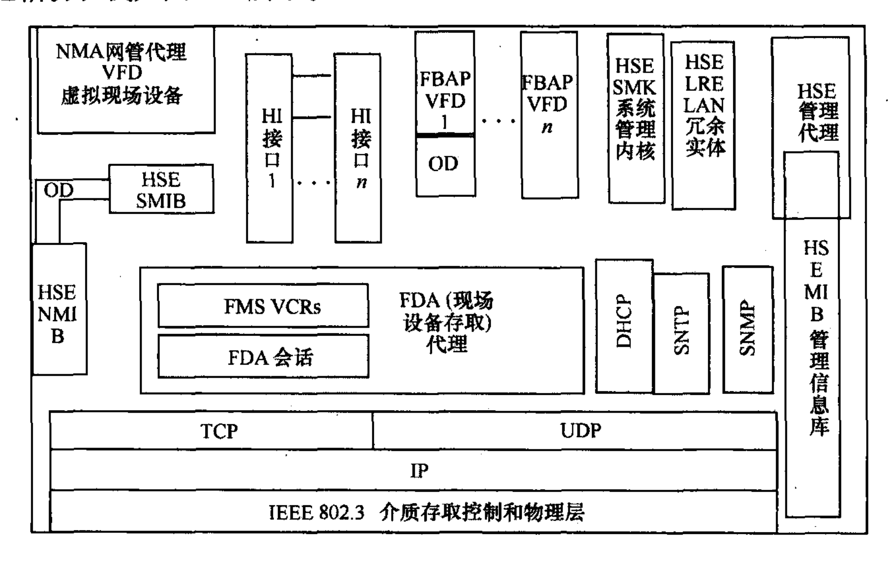


图2.6 HSE的通信协议栈

2.2.2 以太网协议

以太网协议是由一组IEEE 802.3标准定义的局域网协议集。在以太网标准中，有两种操作模式：半双工和全双工。半双工模式中，数据是通过在共享介质上采用载波监听多路访问/冲突检测（CSMA/CD）协议实现传输的。它的主要缺点在于有效性和距离限制，链路距离受最小MAC帧大小的限制。该限制极大地降低了其高速传输的有效性。因此，引入了载波扩展技术来确保千兆位以太网中MAC帧的最小长度为512B，从而达到了合

理的链路距离要求。

当前定义在光纤和双绞线上的传输速率有 4 种:10Mb/s - 10 Base - T 以太网;100Mb/s - 快速以太网;1000Mb/s - 千兆位以太网(802.3z);10 千兆位以太网 - IEEE 802.3ae 以太网。802.3ae 以太网系统由 3 个基本单元组成,各单元功能如下:

(1)物理介质。用于传输计算机之间的以太网信号。

(2)介质访问控制规则。嵌入在每个以太网接口处,从而使得计算机可以公平地使用共享以太网信道。

(3)以太帧。由一组标准比特位构成,用于传输数据。

在所有 IEEE 802 协议中,ISO 数据链路层被划分为两个 IEEE 802 子层,介质访问控制(MAC)子层和 MAC - 客户端子层。IEEE 802.3 物理层对应于 ISO 物理层。MAC 子层有两个基本职能:

(1)数据封装。包括传输之前的帧组合和接收中、接收后的帧解析/差错检测。

(2)介质访问控制。包括帧传输初始化和传输失败恢复。

介质访问控制(MAC) - 客户端子层可能是以下一种:

(1)逻辑链路控制(LLC)。提供终端协议栈的以太网 MAC 和上层之间的接口,其中,LLC 由 IEEE 802.2 标准定义。

(2)网桥实体。提供 LANs 之间的 LAN - to - LAN 接口,可以使用同种协议(如以太网到以太网)和不同的协议(如以太网到令牌环)之间。网桥实体由 IEEE 802.1 标准定义。

10/100Mb/s 以太网中的基本 IEEE 802.3 MAC 数据格式如表 2.1 所列。

表 2.1　IEEE 802.3 MAC 数据格式

7	1	6	6	2	46B ~ 1500B	4B
Pre	SFD	DA	SA	Length Type	Data unit + pad	FCS

Pre(Preamble) - 7B:Pre 字段中 1 和 0 交互使用,接收站通过该字段知道导入帧,并且该字段提供了同步化接收物理层帧接收部分和导入比特流的方法。

SFD(Start - of - Frame Delimiter) - 1B:字段中 1 和 0 交互使用,结尾是两个连续的 1,表示下一位是利用目的地址的重复使用字节的重复使用位。

DA(Destination Address) - 6B:DA 字段用于识别需要接收帧的站。

SA(Source Addresses) - 6B:SA 字段用于识别发送帧的站。

Length/Type - 2B:如果是采用可选格式组成帧结构时,该字段既表示包含在帧数据字段中的 MAC 客户机数据大小,也表示帧类型 ID。

Data 是一组 $n(46 \leq n \leq 1500)$ 字节的任意值序列:帧总值最小为 64B。

FCS(Frame Check Sequence) - 4B:该序列包括 32 位的循环冗余校验(CRC)值,由发送 MAC 方生成,通过接收 MAC 方进行计算得出以校验被破坏的帧。

包含千兆位载波扩展的 MAC 帧:1000 Base - X 最小帧大小为 416B;1000 Base - T 最小帧大小为 520B。通过扩展字段可以满足长度小于最小值的帧需求。

2.2.3　以太网协议与 TCP/IP 协议栈的关系

网络系统是一个庞大而复杂的系统。网络技术发展的初期,主要考虑的问题是如何

进行网络硬件的设计，后来随着网络硬件技术的不断成熟，如何进行网络软件系统的设计就显得越来越重要了。对一个复杂系统进行分析和设计时，常用的方法是“分而治之”，即把一个大的问题分解成若干个子问题或子部分进行设计，然后把它们有机地组织在一起，完成对整个系统的设计。把这个思想应用到网络软件的设计上，人们将网络系统的软件按层的方式来划分。一个网络系统分解成若干个层，一般少的可分成 4 层，多的则可达 7 层，每层负责不同的通信功能，每一层好像一个“黑匣子”，它内部的实现方法对外部的其他层来说是透明的，每层都向它的上层提供一定的服务，同时可以使用它的下层所提供的功能，这样，在相邻层之间就有个接口把它们联系起来。显然，只要保持相邻层之间的接口不变，一个层内部可以用不同的方式来实现。一般把网络的层次结构和每层所使用协议的集合称为网络体系结构，一个具体的网络系统所包含的层数和每层所使用的协议是确定的。在这种层次结构中，各层协议之间形成了一个从上到下类似栈的结构的依赖关系，通常叫协议栈。

TCP/IP 协议的体系结构分为 4 层，由高到低分别为应用层、传输层、网络层和链路层，如表 2.2 所列。

表 2.2　TCP/IP 各层协议

体系结构	协　议
应用层	Telnet、FTPXHTTP、DNSSNMP 和 SMTP 等
传输层	TCP 和 UDP
网络层	IP、ICMP 和 IGMP
链路层	以太网、令牌环网、FDDI、IEEE802.3 等

TCP/IP 各层协议中，每一层完成不同的通信功能，各层具体功能和所包含的协议说明如下。

1. 链路层

链路层在 TCP/IP 协议栈的最低层，也称为数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。链路层的功能是把接收到的网络层数据报（也称 IP 数据报），通过该层的物理接口发送到传输介质上，或从物理网络上接收数据帧，抽出 IP 数据报并交给 IP 层。TCP/IP 协议栈并没有具体定义链路层，只要是在其上能进行 IP 数据报传输的物理网络如以太网、令牌环网、FDDI（光纤分布数据接口）、IEEE 802.3 及 RS－232 串行线路等，都可以当成 TCP/IP 协议栈的链路层。这样做的好处是 TCP/IP 协议可以把重点放在网络之间的互联上，而不必纠缠物理网络的细节，并且可以使不同类型的物理网络互联。也可以说，TCP/IP 协议支持多种不同的链路层协议。ARP 地址解析协议和 RARP 逆地址解析协议是某些网络接口使用的特殊协议，如以太网和令牌环网，用来进行网络层地址和网络接口层地址（物理地址）的转换。

2. 网络层

网络层也称为互联网层，由于该层的主要协议是 IP 协议，因而也可简称为 IP 层。它是 TCP/IP 协议栈中最重要的一层，主要功能是可以把源主机上的分组发送到互联网中

的任何一台目的主机上。可以想象,由于在源主机和目的主机之间可能有多条通路相连,因而网络层就要在这些通路中做出选择,即进行路由选择。在 TCP/IP 协议族中,网络层协议包括 IP 协议、ICMP 协议以及 IGMP 协议。

3. 传输层

通常所说的两台主机之间的通信其实是两台主机上对应应用程序之间的通信,传输层提供的就是应用程序之间的通信,也叫端到端(End - to - End)的通信。在不同情况下,应用程序之间对通信质量的要求是不一样的。因此,在 TCP/IP 协议族中传输层包含传输控制协议(TCP)和用户数据报协议(UDP)。

TCP 为两台主机提供高可靠性的数据通信,当有数据要发送时,它对应用程序送来的数据进行分片,以适合网络层进行传输:当接收到网络层传来的分组时,它对收到的分组要进行确认;它还要对丢失的分组设置超时重发等。由于 TCP 提供了高可靠性的端到端通信,因此应用层可以忽略所有这些细节,以简化应用程序的设计。

UDP 则为应用层提供一种非常简单的服务,它只是把称作数据报的分组从一台主机发送到另一台主机,但并不保证该数据报能正确到达目的端,通信的可靠性必须由应用程序来提供。用户在自己开发应用程序时可以根据实际情况,使用系统提供的接口函数方便地选择是使用 TCP 还是 UDP 进行数据传输。

4. 应用层

应用层向使用网络的用户提供特定的、常用的应用程序,如使用最广泛的远程登录(Telnet)、文件传输协议(FTP)、超文本传输协议(HTTP)、域名系统(DNS)、简单网络管理协议(SNMP)和简单邮件传输协议(SMTP)等。要注意有些应用层协议是基于 TCP 协议的,如 FTP 和 HTTP 等;有些应用层协议是基于 UDP 协议的,如 SNMP 等。

TCP/IP 协议 4 层结构中有两个重要的边界:一个是将操作系统与应用程序分开的边界;另一个是将高层互联网地址与低层物理网卡地址分开的边界。TCP/IP 协议模型的两个边界如图 2.7 所示。

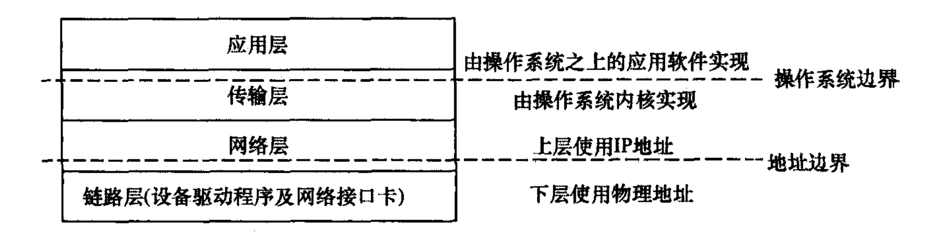


图 2.7　TCP/IP 协议模型的两个边界

操作系统边界的上面是应用层,应用层处理的是用户应用程序的细节问题,提供面向用户的服务。这部分的程序一般不包含在操作系统内核中,由一些独立的应用程序组成,本书中设计的网络程序就属于这一层,操作系统边界的下面各层包含在操作系统内核中,是由操作系统来实现的,它们共同处理数据传输过程中的通信问题。

地址边界的上层为网络层,网络层用于对不同的网络进行互联,连接在一起的所有网络为了能互相寻址,要使用统一的互联网地址。而地址边界的下层为各个物理网络,不同的物理网络使用的物理地址各不相同,因此,在地址边界的下面只能是各个互联起来的网络使用自己能识别的物理地址。

2.2.4　嵌入式以太网技术的优势

以太网将是未来测控网络的最佳解决方案，与其他类型的总线网络相比，具有如下明显优势。

人们对以太网技术十分熟悉，可以显著降低系统的开发、培训和维修费用。同时，由于应用广泛，其硬件价格和安装成本均十分低廉，以太网网卡的价格只有 Profibus FF 等现场总线网卡的 1/10。

以太网传输速率高，目前 1000Mb/s 的以太网已开始广泛应用，1000Mb/s 以太网也逐渐成熟，其速率比目前的现场总线快得多。交换式以太网效率高，利用实时以太网技术使其实时性与确定性均能满足测试的要求。

以太网具有彻底的开放性，能与世界上主要的计算机平台和 Microsoft Windows 兼容。由于采用标准协议，因此来自许多供应商的设备在同一网上可共存及相互间通信。以太网可以满足控制系统各个层次的要求，且易于与因特网集成，使企业信息网络与测控网络易于集成。

以太网能够完全胜任测控环境中对可靠性和抗干扰性的严格要求。现代以太网采用非屏蔽双绞线，它的抗干扰能力与 4mA ~ 20mA 模拟传输线路相当，若采用屏蔽双绞线或光纤通信则具有更强的抗干扰能力。

2.3　基于以太网的智能网络传感器硬件结构

2.3.1　硬件平台通用总体结构

不同的测试任务决定了测试系统的结构和智能网络传感器结构：在测控点较多、测量数据量较多时，可以考虑用 32 位微处理器直接扩展测控外部设备；在测控点较多、测量数据量不多时，可将距离较近的测试点通过传统的现场总线相连，用高性能微处理器作为信号级网关，在现场总线和测控专用网之间进行协议转换；在测量点较少或测控点分布超出现场总线的连接距离的情况下，可以用 8 位或 32 位微处理器直接扩展测控外部设备。

根据网络容量、传输速率、数据处理需求和计算能力的应用需要，可选择不同配置的微处理器和 10Mb/s 或 100Mb/s 的以太网控制器，如图 2.8 所示。如果数据量比较大，信号交联复杂，也可以通过采用如图 2.8 所示的 DSP 加上微控制器的结构，实现普通设备的网络接入能力。

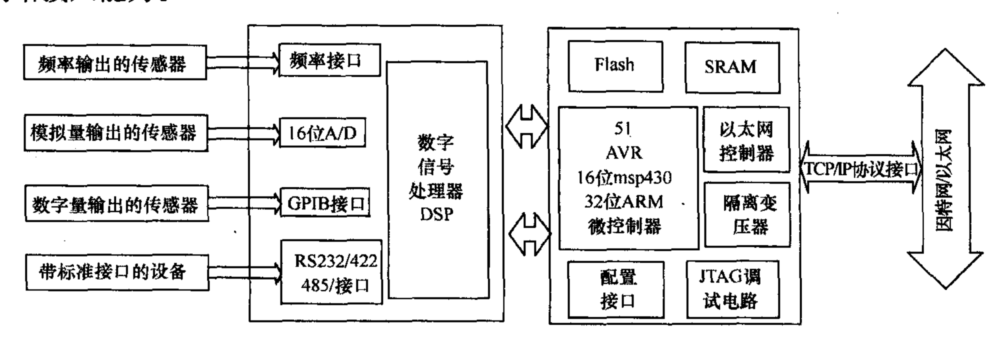


图 2.8　嵌入式以太网传感器硬件通用结构

基于 DSP 的硬件模块对符合总线协议的数据流进行实时采集和处理,并封装成 TCP 或 UDP 数据报,微控制器模块负责全系统的通信并将上述数据报传送到以太网。在硬件构成上,可以实现 ARM 核的微控制器作为主处理器,完成系统管理及网络传输;DSP 作为协处理器,完成信号处理、分析、信息融合。DSP 的快速数据处理能力和 ARM 良好的网络通信能力保证了测试数据实时高效地传送给远端用户。

作为嵌入式微控制器的运算单元,可以选择 8/16/32 位的微控制器、数字信号处理器(DSP)和可编程逻辑器件(FPGA 或 CPLD)。目前,典型微控制器芯片有 8 位 51 内核单片机 P89V51RD2,AVR 系列单片机 Atmega128L 和 32 位 ARM 核微控制器 LPC2210、2220、2230 等。

以太网控制器是实现数据流传入以太网的硬件平台,即通常所说的网卡芯片,与在 PC 机上使用的网卡芯片不同,在设计嵌入式智能网络传感器中通常有全双工 RTL8019AS、全双工 CS8900A 和全双工 DM9000E。

2.3.2　存储设备

RAM 能够随时在任一地址读出或写入内容。RAM 的突出优点是读/写方便、使用灵活;缺点是不能长期保存信息,一旦停电,所存信息就会丢失。所以,RAM 用于二进制信息的临时存储或缓冲存储,在嵌入式系统中主要用于以下几方面:

(1)存放当前正在执行的程序和数据,如用户的调试程序、程序的中间运算结构以及掉电时无需保存的 I/O 数据和参数等。

(2)作为 I/O 数据缓冲存储器,如显示输出缓冲存储器、键盘输入缓冲存储器等。以显示缓冲存储器为例,它实质上就是在主存中开辟的一个存放字符、汉字、图形、图像等显示信息的数据缓冲区。

(3)作为中断服务程序中保护 CPU 现场信息的堆栈。

随机存储器由两大类组成:静态随机存储器(Static RAM,SRAM)和动态随机存储器(Dynamic RAM,DRAM)。下面具体分析这两种随机存储器的结构特征。

2.3.2.1　静态随机存储器

SRAM 的存储单元电路是以双稳态电路为基础的,因此状态稳定,只要不掉电,信息就不会丢失。SRAM 的接口和操作时序如图 2.9 所示。

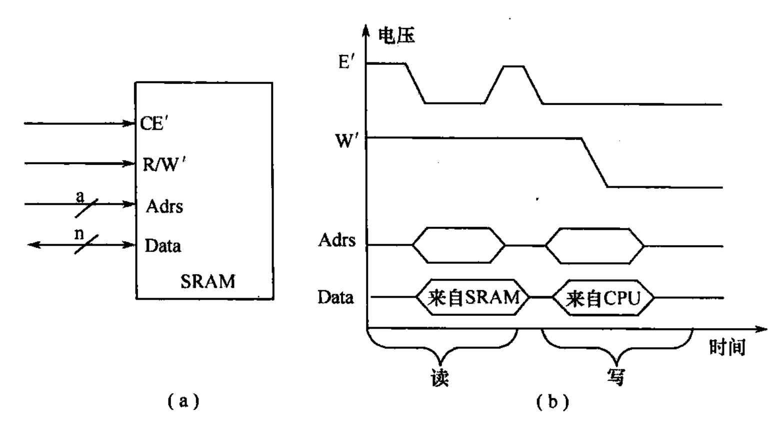


图 2.9　SRAM 的接口电路与操作时序

CE′是芯片启用输入，在低电平工作。当 CE′ = 1 时，SRAM 的 Data 引脚被禁用；当 CE′ = 0 时，SRAM 的 Data 引脚被启用。

R/W′控制当前操作是读（R/W′ = 1）还是写（R/W′ = 0）。读/写是相对于 CPU 而言的，因此读意味着从 RAM 读，写意味着写至 RAM。需要注意的是，有些 SRAM 的读/写使用两个控制引脚即 WR′和 RD′时执行写操作；RD′ = 0 时执行读操作。

Adrs 指出读或写的地址。

Data 是数据传输双向信号束。R/W′ = 1 时，该引脚为输出；R/W′ = 0 时，该引脚为输入。

SRAM 的操作方法有两种，即读操作和写操作。

SRAM 上读操作的方法如下：当 R/W′ = 1 时，让 CE′ = 0，启用 SDRAM。将地址送到地址线上。一定延迟时间后，数据通过数据线进行传输。

SRAM 上写操作的方法如下：让 CE′ = 0。启用 SDRAM。让 R/W′ = 0。地址出现在地址线上，数据出现在数据线上。

在使用 SRAM 时，需要考虑 SRAM 与处理器的匹配，一般包括工作电压、工作速度、时序等的匹配。电路设计完成把 SRAM 接到系统总线上的工作。

2.3.2.2　动态随机存储器

DRAM 的存储单元电路是以电容为基础的，电路简单，集成度高，功耗小。但是 DRAM 即使不掉电也会因电容放电而丢失信息，需要定时刷新，因此在工作时必须配合 DRAM 控制器。DRAM 控制器是位于处理器和存储器芯片之间的一个额外的硬件，如图 2.10 所示。它的主要用途是执行 DRAM 的刷新操作，使得 DRAM 中数据有效。



图 2.10　DRAM 存储器系统

DRAM 的接口和读写时序有其自身的特点，如图 2.11 所示。DRAM 芯片集成度高，存储容量大，导致引脚数量不够，因此地址输入采用两路复用锁存方式。也就是说，DRAM 将地址信号分为两组，共用几根地址输入线，分两次把地址送入芯片内部锁存起来。这两组地址信号的送入，分别用行地址选择（RAS′）和列地址选择（CAS′）控制。读操作的时序图表明地址按以下两步提供：首先，RAS′置成 0，地址的行部分（即地址高位部分）置于地址线；然后，CAS′置成 0，地址的列部分（即地址低位部分）置于地址线。

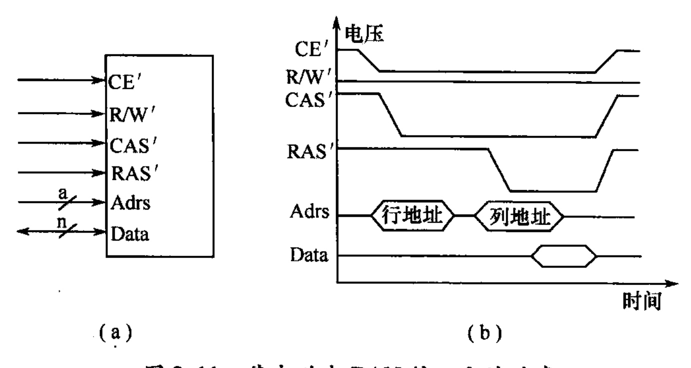


图 2.11　基本动态 RAM 接口和读时序

2.3.2.3　RAM 的选择

在设计嵌入式系统时选择何种存储器，通常考虑以下因素：如果系统的随机存储器的容量不是很大，则一般采用 SRAM；反之，选择 DRAM。对于特别高速度的应用，使用 SRAM。如果嵌入式系统对功耗敏感，可使用 SRAM。因为 DRAM 需要定时刷新，功耗相对大，而 SRAM 在系统进入待机工作方式时，只需要微小的待机电流即可维持数据不丢失。需要注意的是，SRAM 的平均功耗低，但是工作时功耗不一定低。

对于嵌入式处理器而言，有的嵌入式处理器芯片集成了 DRAM 控制器，这时选择 DRAM 比较好。一般地，小规模的嵌入式系统不建议使用分离的 DRAM 控制器 + DRAM 的方案，因为这种方案既会增加系统的复杂性，如电路板的面积、故障率等，又会增加系统的成本。因此，如果选用了 DRAM，那么尽量使用带有 DRAM 控制器的嵌入式处理器，然后配合使用 DRAM。

目前，基于 32 位嵌入式处理器的嵌入式系统一般使用 DRAM。复杂的嵌入式系统可以采用 SRAM 和 DRAM 混合设计的方案。不同要求的数据使用不同的随机存储器，以满足系统整体的优化设计。嵌入式系统的设计，在使用 SRAM 和 DRAM 的成本上，需要仔细并与整个系统的硬件一起进行核算，最终做出选择。在选择存储器类型时，一般要考虑存取时间和成本。SRAM 提供了极快的存取时间，一般比 DRAM 快 4 倍，但是造价十分昂贵。通常，SRAM 只是用于那些存取速度极端重要的场合。在需要使用大容量的 RAM 时，一般选择使用 DRAM。很多嵌入式系统混合使用两种 RAM，如关键数据通道上的一小块 SRAM（几百至几千个字节）和其他所有地方的一大块 DRAM（以兆计）。

Flash Memory（按块擦除存储器）是存储器技术的最新发展，它综合了目前为止所有存储器器件的优点，主要特点是在不加电情况下能长期保存信息，同时又能在线进行快速擦除与重写。从软件的观点来看，Flash Memory 和 EEPROM 的技术十分类似。但是 EEPROM 擦写和编程时要加高电压，这意味着重新编程时必须将芯片从系统中取出。而 Flash Memory 使用标准电压擦写和编程，允许芯片在标准系统内部编程。这就允许 Flash Memory 在重新编程的同时存储新的内容。此外，EEPROM 必须被整体擦写，Flash Memory 可以一块一块地擦写。大部分 Flash Memory 允许某些块被保护，这一点对存储空间有限的嵌入式系统非常有用。例如，可将引导代码放进保护块内，而允许更新设备上其他的存储器块。

理想的存储器应具有密度高、读/写速度快、价格低和非易失性的特点。但是，传统的存储器却只能满足这些要求中的一部分。Flash Memory 的推出，恰好同时实现了所有这些优良的存储器特性。Flash Memory 是一种高密度、低价格的高性能读/写存储器，兼有功耗低、可靠性高等特点。表 2.3 所列为 Flash Memory 与传统存储器技术的比较。

表 2.3　Flash Memory 与传统存储器技术的比较

存储器	固有不发挥性	高密度	低功耗	单晶体管单元	在线可重写
Flash Memory	√	√	√	√	√
SARM					√
DRAM		√			√
EPROM	√	√	√		•
EEPROM	√		√	√	
掩膜 ROM	√	√	√	√	

根据工艺的不同,Flash Memory 主要有两类:NOR Flash Memory 和 NAND Flash Memory。NOR Flash Memory 是在 EEPROM 的基础上发展起来的,它的存储单元由 N-MOS 构成,连接 N-MOS 单元的线是独立的。NOR Flash Memory 的特点是可以随机读取任意单元的内容,适合于程序代码的并行读/写、存储,所以常用于制作计算机的 BIOS 存储器和微控制器的内部存储器等。NAND Flash Memory 是将几个 N-MOS 单元用同一根线连接来,可以按顺序读取存储单元的内容,适合于数据或文件的串行读/写。Flash Memory 的操作包括写入和读出。

读操作:从 Flash Memory 中读出数据与其他存储器的操作基本相同。处理器只要提供地址、读操作信号和片选信号,存储器就返回在该位置保存的数据。大部分的 Flash Memory 在系统重启时自动进入读状态,启动读状态不需要特别的初始化序列。

写操作:把程序或数据写入 Flash Memory 的过程叫做编程。Flash Memory 的编程有两种方式,一种是在线编程,一种是离线编程。Flash Memory 的编程操作比较麻烦,主要表现在以下 3 个方面。

(1)每一个存储位置必须在重写操作之前被擦除。如果旧的数据没有被擦除,那么写操作的结果会是新、旧数值的某种逻辑组合,存储的数据通常是错误的。

(2)一次只能有一个扇区或者块被擦除,而且不可能只是擦除一个单个的字节。

(3)擦除旧数据的过程和写入新数据的过程是随制造商的不同而变化的。因此在进行 Flash Memory 写入操作时,提供一个软件层来完成写入和擦除操作比较方便,这个软件叫做 Flash Memory 的驱动程序。

设计 Flash Memory 驱动程序的目的是为了屏蔽不同制造商提供的器件在写入操作时的细节,为上层软件设计提供一个统一的接口,以便于上层软件的移植和开发。Flash Memory 的驱动程序应该有一个由擦除和写操作组成的简单应用编程接口。当需要修改 Flash Memory 中的数据的部分应用软件时,只要调用驱动程序来控制细节即可。这样就允许应用程序员做一个高级的请求,如擦除地址 D0000H 处的块或于地址 D0000H 处开始写入一块数据。通过设计并使用 Flash Memory 的设备驱动程序,当使用其他制造商的 Flash Memory 时,软件代码可以很容易地被修改。

2.4 基于以太网的智能网络传感器软件结构

基于以太网的嵌入式智能网络传感器软件体系结构需要采用层次化、结构化和组件化的设计原则,结合面向远程网络应用需求,深入分析相关关键技术后,构建并论证软件平台的总体结构、功能组成和实现方法,为具体软件模块的功能实现提供指导方法,如图 2.12 所示。

在该软件平台体系结构最下层的为构成嵌入式智能网络传感器硬件系统的各种元器件的驱动程序,如微控制器引导程序、网卡驱动程序、传感器接口程序和板级支持包等;第二层为属于嵌入式操作系统范畴的核心模块,对下操作和管理硬件资源,对上服务于各种应用任务;第三层为总线协议/数据中间件和嵌入式 TCP/IP 协议栈,用于进一步屏蔽下层操作系统级的软件差异,为硬件平台的可移植性提供平滑过渡,同时为上层的 TCP/UDP 服务器和 Web 服务器的应用提供网络支持。

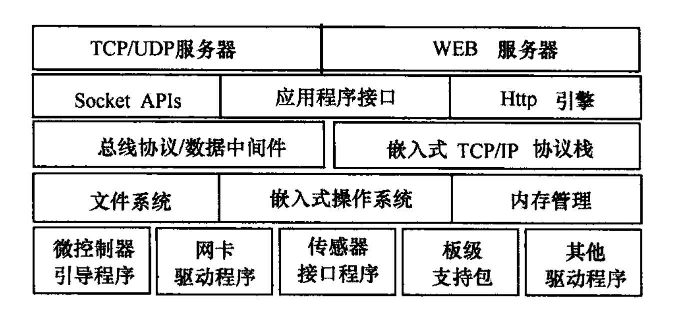


图2.12 嵌入式智能网络传感器软件体系结构

2.4.1 硬件模块驱动程序设计

硬件模块驱动程序的设计主要可以分为硬件平台 BootLoader 程序和设备驱动程序两大类。

2.4.1.1 BootLoader 开发

BootLoader 是系统加电后首先运行的一段程序代码,其目的是将系统的软硬件环境带到一个合适的状态,为调用操作系统内核准备好正确的环境。对于不使用操作系统的嵌入式系统而言,应用程序的运行同样也需要依赖这样一个准备良好的软硬件环境,因此从这个意义上来讲,BootLoader 对于嵌入式系统是必需的。

BootLoader 是依赖于目标硬件实现的,可以从以下两个方面来理解:

(1)每种嵌入式微处理器体系结构都有不同的 BootLoader。当然,有些 BootLoader 也可以支持多种体系结构的嵌入式微处理器。例如,U - Boot 可同时支持 ARM 体系结构和 MIPS 体系结构。

(2)BootLoader 还依赖于具体的嵌入式板级硬件设备的配置。也就是说,即使是基于相同嵌入式微处理器构建的不同嵌入式目标板,要想让运行在一个板上的 BootLoader 程序同样运行在另一个板上,也还需要修改 BootLoader 的源程序。

因此,为嵌入式系统建立一个通用、标准的 BootLoader 应该是几乎不可能的。尽管如此,仍然可以归纳一些通用的概念来指导开发人员对 BootLoader 的设计与实现。

【例2.1】以基于 ARM7 TDMI 内核的 S3C4510B 为例,具体介绍 BootLoader 的启动过程。

在启动过程中,BootLoader 依次初始化 CPU 在各种模式下的堆栈空间、设定 CPU 的内存映射、对系统的各种控制寄存器进行初始化、对 CPU 的外部存储器进行初始化、设定各外围设备的基地址、创建正确的中断矢量表、为 C 代码执行创建 ZI(零创建)区,然后进入到 C 代码。在 C 代码中继续对时钟、RS - 232 端口进行初始化,然后打开系统中断允许位。最后进入到应用代码中执行,执行期间响应各种不同的中断信号并调用预先设置好的中断服务程序处理这些中断。整个过程的流程图如图2.13 所示。

2.4.1.2 设备驱动程序

使用任何外部设备都需要有响应驱动程序的支持。驱动程序为上层软件提供设备的操作接口。对于上层软件而言,只需要调用驱动程序提供的接口,而不用理会设备具体的内部操作。对于驱动程序而言,不仅要实现设备的基本功能函数,如初始化、中断响应、发

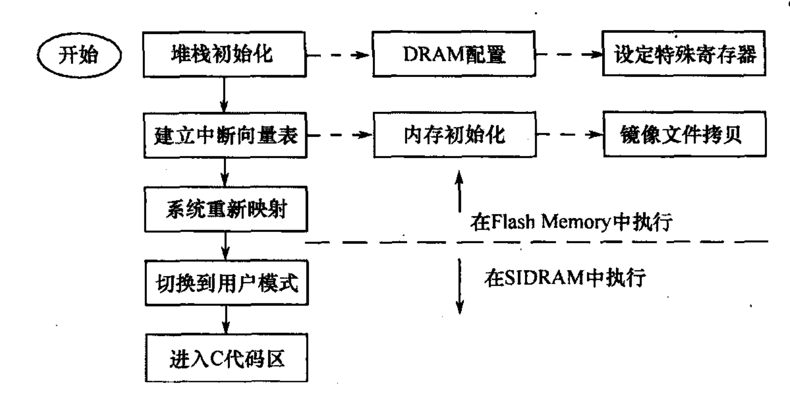


图 2.13　BootLoader 启动流程图

送、接收等，使设备的基本功能得以实现，而且针对设备使用过程中可能出现的各种差错，还应提供完备的错误处理函数。

驱动层软件有两个重要的概念：硬件抽象层（Hardware Abstraction Layer，HAL）和板级支持包（Board Support Package，BSP）。可以简单地理解为硬件抽象层与硬件具有更加紧密的相关性，而板级支持包与操作系统具有更加紧密的相关性[1]。

具体地讲，硬件抽象层的目的是为了将硬件抽象化，即通过程序来控制诸如 CPU、I/O、存储器等硬件的操作，从而使得系统的设备驱动程序与硬件无关。为实现这一目的，在定义抽象层时，需要根据系统需求规定统一的软硬件接口标准。在功能上，抽象层一般应实现相关硬件的初始化、数据的 I/O 操作、硬件设备的配置操作等。引入硬件抽象层的概念可以大大提高系统的可移植性。另外，软硬件的测试工作也都可以基于硬件抽象层来完成，这使得软、硬件测试并行进行成为可能。

设计板级支持包的目的主要是为驱动程序提供访问硬件设备寄存器的函数包，从而实现对操作系统的支持。为保证与操作系统保持正确的接口，以便良好地支持操作系统，不同的操作系统应对应不同定义形式的板级支持包。在功能上。板级支持包大体需要实现以下两方面的内容：

（1）在系统启动时，完成对硬件的初始化，如对设备的中断、CPU 的寄存器和内存区域的分配等进行操作。这部分工作是比较系统化的，要根据 CPU 的启动、嵌入式操作系统的初始化以及系统的工作流程等多方面要求来共同决定这一部分 BSP 应完成的功能。

（2）为驱动程序提供访问硬件的手段。所谓访问硬件，其实质是访问硬件设备的寄存器。如果系统是统一编址的，则可以直接在驱动程序中用 C 语言的函数进行访问。如果系统是单独编址的，则 C 语言就不能够直接访问，只有用汇编语言编写的函数才能进行访问。而板级支持包就是这种为上层的驱动程序提供访问硬件设备寄存器的函数包。

在对硬件进行初始化时，BSP 一般应完成以下工作：

（1）将系统代码定位到 CPU 将要跳转执行的内存入口处，以便在硬件初始化完毕后 CPU 能够执行系统代码。此处的系统代码可以是嵌入式操作系统的初始化入口，也可以是应用代码的主函数入口。

（2）根据不同 CPU 在启动时的硬件规定，BSP 要负责将 CPU 设置为特定状态。

（3）对内存进行初始化，根据系统的内存配置将系统的内存划分为代码、数据、堆栈等不同的区域。

(4)如果有特殊的启动控制代码,则 BSP 要负责将控制权移交给启动控制代码。例如,在某些场合,系统为了减少存储所需的 ROM 容量而进行压缩处理,那么在系统启动时要先跳转到一段控制代码,它将系统代码进行解压后才能继续系统的正常启动。

(5)如果应用软件中包含一个嵌入式操作系统,则 BSP 要负责将操作系统需要的模块加载到内存中。嵌入式应用软件系统在进行固化时,可以有基于 ROM 的和常驻 ROM 的两种方式,在基于 ROM 方式时,系统在运行时要将 ROM 或 Flash Memory 内的代码全部加载到 RAM 内;在常驻 ROM 方式时,代码可以在 ROM 或 Flash Memory 内运行,系统只将数据部分加载到 RAM 内。

(6)如果应用软件中包含一个嵌入式操作系统,则 BSP 还要在操作系统初始化之前,将硬件设置为静止状态,以避免造成操作系统初始化失败。

2.4.2　嵌入式操作系统

随着嵌入式应用的日益广泛,程序设计也越来越复杂,这就需要一个操作系统来对其进行管理和控制。复杂系统常常使用嵌入式操作系统,这样的系统一般可以扩展程序存储器,资源相对较多,系统实现的功能比较复杂,软件开发的工作量和开发的难度比较大,维护费用比较高。使用嵌入式操作系统可以有效地提高这些系统的开发效率[2]。

嵌入式系统采用的操作系统一般是实时操作系统(Real Time Operating System, RTOS),它是嵌入式应用软件的基础和开发平台。RTOS 一般是一段嵌入在目标代码中的软件,用户的其他应用程序都建立在它的基础上。RTOS 的引入,解决了嵌入式软件开发标准化的难题。随着嵌入式系统中软件比重不断上升、应用程序越来越大,对开发人员、应用程序接口、程序档案的组织管理成为一个大的课题。引入 RTOS 相当于引入了一种新的管理模式,对于开发单位和开发人员都是一个提高。基于 RTOS 开发出的程序,具有较高的可移植性,可以实现 90% 以上的设备独立,一些成熟的通用程序还可以作为专用库函数产品推向社会。嵌入式软件的函数化、产品化能够促进嵌入式软件模块的复用性,从而降低系统的研发成本。

【例 2.2】以 μC/OS - II 为例,μC/OS - II 是一个完整的、源码公开的、可移植、固化、裁剪的占先式实时多任务内核,主要面向中小型嵌入式系统,具有执行效率高、占用空间小、可移植性强、实时性能优良和可扩展性强等特点。

μC/OS - II 结构小巧,最小内核可编译至 2KB,即使包含全部功能,编译后也仅有 6KB ~ 10KB,因而非常适用于小型控制系统。μC/OS - II 具有良好的兼容性,如系统本身不支持文件系统,但是如果需要,也可以自行加入文件系统的内容。此外,μC/OS - II 是用 ANSI 的 C 语言编写的,包含一小部分汇编语言代码,使之可供不同架构的微处理器使用。至今,从 8 位到 16 位,μC/OS - II 已在超过 49 种不同架构的微处理器上成功移植。

μC/OS - II 的软件体系结构以及与硬件的关系如图 2.14 所示,其软件体系主要包括以下 4 个部分:

(1)应用软件层。在应用程序中使用 μC/OS - II 时,用户开发设计的应用代码。

(2)与应用相关的配置代码。与应用软件相关的、μC/OS - II 的配置代码。包括两个头文件,这两个头文件分别定义了与应用相关的控制参数和所有相关的头文件。

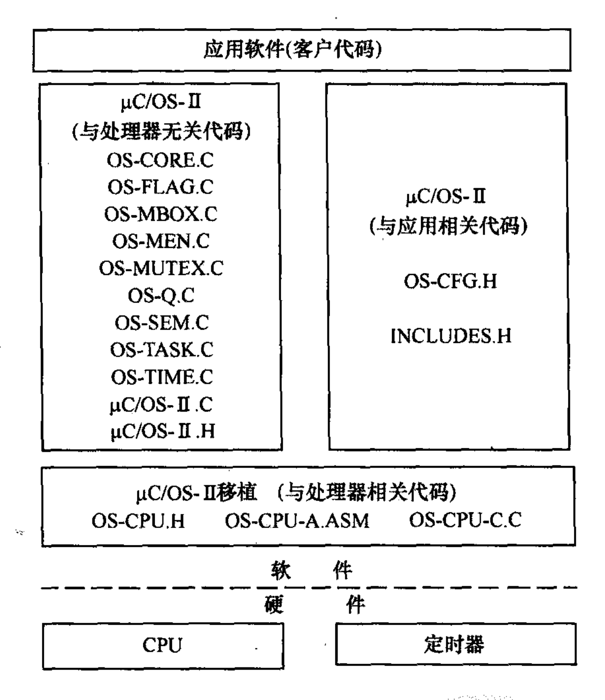


图 2.14　μC/OS－Ⅱ的软件体系结构以及与硬件的关系图

(3)与处理器无关的核心代码。包括与处理器无关的 10 个源代码文件和 1 个头文件。其中,10 个源代码文件分别实现了 μC/OS－Ⅱ内核结构,即内核管理、事件管理、消息邮箱管理、内存管理、互斥型信号量管理、消息队列管理、信号量管理、任务管理、定时管理和内核管理。

(4)与处理器相关的设置代码。与处理器相关的源代码,包括 1 个头文件、1 个汇编文件和一个 C 文件。在不同处理器上移植 μC/OS－Ⅱ时,需要根据处理器的类型对这部分代码重新编写。可以在 μC/OS－Ⅱ的网站 www. μC/OS－Ⅱ. com 中查找移植范例,也可以阅读处理器的移植代码进行编译。

2.4.3　嵌入式 TCP/IP 协议栈

嵌入式协议栈的运行必须基于嵌入式操作系统平台的支持,但并不是说协议栈必须依赖于嵌入式操作系统的 API。实际上,许多嵌入式协议栈做到了相对于操作系统的最大独立性,可以与大多数嵌入式操作系统集成运行。但是,协议栈以及附带的上层接口和下层驱动程序会给嵌入式系统设计设置其他的约束。例如,TCP/IP 协议栈必须有一个相对的准确时间源,以便进行时间管理,处理各种发生在栈中的超时和定时行为。此外,协议栈还必须包含一个资源管理系统。这个系统可能是一个标准的动态存储管理系统,也可能是为速度预先分配包缓存的客户系统。

目前,嵌入式协议栈的提供有两种方式:一种是独立的第三方协议栈产品;另一种嵌入式操作系统提供商提供协议栈产品。后一种方法在开发时相对要简单些,而且能够提供较强的软件可使用性[3]。

建立基于网络的嵌入式系统需要根据具体的应用环境和使用的网络技术来选择适合

的网络协议栈。例如,如果开发的嵌入式产品是基于网络的打印机,且能够通过 Novell 服务器存取,那么就必须采用 Netware 打印协议的协议栈;如果设计的打印机要从尽可能多的网络访问,则最好选择 TCP/IP 协议栈,因为 TCP/IP 是应用最广泛的协议;如果设计的打印机同时支持 TCP/IP 和 Netware 协议,那么打印机就既可以通过 TCP/IP 存取,也可以通过 Netware 局域网络存取。

为嵌入式系统选择网络协议栈需要从以下 3 个方面考虑:

(1)网络协议占用的内存。对于一个网络协议栈组件,占用的内存主要表现在两个方面。一个是协议栈代码段占用的存储器的大小;另一个是数据段占用的存储器的大小。其中,数据段包括普通数据段和堆栈段对存储器的占用。选择协议栈时,需要对协议栈占用的内存进行估计。例如,对于常用的 TCP/IP 协议栈,不同的商家提供的产品不同。有的用于 PC 机的协议栈产品不一定适合嵌入式系统应用,因为 PC 机使用的协议栈可能不考虑对内存的占用,而嵌入式系统对内存的要求比较苛刻。通常厂家会提供这一指标,如 Interniche 的协议栈占用内存大约为 50KB。

(2)硬件资源。硬件资源主要指的是与网络有关的部件,如通信控制器、物理层接口等。在选择网络组件时,需要考虑这些硬件资源的成本因素。有时还需要考虑集成和分离两种设计方法的实现成本等因素。

(3)协议开销。协议开销指的是 CPU 运行协议栈产生的开销。添加网络支持可能会导致系统实时响应的延迟。有时还需要对嵌入式处理器进行升级,从而导致系统成本增加。

一般情况下,嵌入式协议栈与嵌入式操作系统是集成在一起的,购买集成的嵌入式协议栈时,商家可以提供集成系统的综合指标。

嵌入式 TCP/IP 协议栈完成的功能与完整协议栈是相同的,但是由于嵌入式系统的资源有限,嵌入式协议栈的一些指标和接口可能与普通的协议栈不同,这体现在以下几个方面:

(1)嵌入式协议栈的 API 可能与普通的协议栈不同。普通嵌入式的接口是标准的,如 winsock、BSD socket 等,标准化的优点是可实现应用软件的兼容性,但是带来的问题是为了实现标准化的接口必然使用了大量的代码,不仅效率低,而且处理器和存储器的开销大。当然,也有许多厂商将标准的协议栈接口移植到嵌入式系统中。于是,建立在 Berkeley socket 上的协议栈也称为嵌入式的。但是,Berkeley 栈带来许多台式机所需要的特性,而这些特性对于嵌入式的应用是不需要的。总之,建立在专用 socket 基础上的协议栈效率比较高,但是它提供的 API 与通用插座协议栈 API 有所不同。

(2)嵌入式协议栈的可裁剪性。普通协议栈使用协议栈的全集,只是因为普通计算机的资源丰富。对于资源有限的嵌入式系统来说,可裁减性非常重要。例如,TCP/IP 协议中,UDP 和 TCP 属于传输层协议。TCP 是面向连接的、传输可靠的协议。为了保证到达数据的准确无误,TCP 采用校验和的方式来检查数据是否有错误或有丢失,如果发现存在问题的要求重发。再者,TCP 协议在应用层上保证到达数据的前后次序无误,接收数据的节点负责恢复数据的顺序。而 UDP 是无连接的、不能保证可靠传输的协议,UDP 仅仅把校验和作为选项,也不保证数据的顺序,不存在重发的必要,所以它的效率比较高。因此,这两种协议有不同的用途。如果通信系统通道对于可靠性的要求不太高,但是对实时

性和效率要求比较高,则可以选用UDP。UDP比较适合于传输媒体本身十分可靠的情况,此时不需要采用TCP协议那样的服务程序,从而减少了系统的负担。

(3)嵌入式TCP/IP协议栈的平台兼容性。通常,普通协议栈与操作系统的结合比较紧密,协议栈的实现依赖于操作系统提供的服务,移植起来一般比较困难。但是,嵌入式协议栈设计一般对操作系统的依赖性不大,便于移植,许多商用的嵌入式TCP/IP协议栈支持多种操作系统平台,或者需要很少的移植代码。

(4)嵌入式协议栈的效率较高。主要体现在占用的代码空间小、需要的数据存储器小、代码的效率高,从而可以减少对处理器的处理速度的要求。

参考文献

[1] Jing Bo, Sun Yong, Zhang Jie. A De-noising and Compress Algorithm of Multi-sensor System Based on BP Neural Network. ICEMI/2005,4.

[2] Pardo J, Campelo,J C, Serrano,J J. Robustness study of an embedded operating system for industrial[C]. Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04) Fault Tolerant Systems Group Polytechnic University of Valencia. Spain.

[3] 崔光佐,程旭,等. 面向处理器的系统级模拟、仿真及调试技术——基于软硬件协同设计的新方法[J]. 计算机研究与发展. 2001,38(3):361-367.

第3章　无线智能网络传感器

无线通信技术、集成电路技术、传感器技术以及MEMS等技术的飞速发展与日益成熟,使得低成本、低功耗、多功能的微型传感器的大量生产与应用成为可能。这些传感器在微小体积内通常集成了信息采集、数据处理和无线通信等多种功能。而无线通信使灵活性、简洁性、大规模的网络化工程实施成为可能。以往的有线组网存在诸多不足,投资和使用成本过高,2001年全球工业用传感器的市场份额是110亿美元,而安装和使用成本超过1000亿美元,从图3.1中可以很直观的看出有线网络组网的弊端。因此,基于应用需求和相关技术的不断发展,无线智能网络传感器应运而生,并且随着时间地推移,无线智能网络传感器将发挥出越来越强有力的作用。

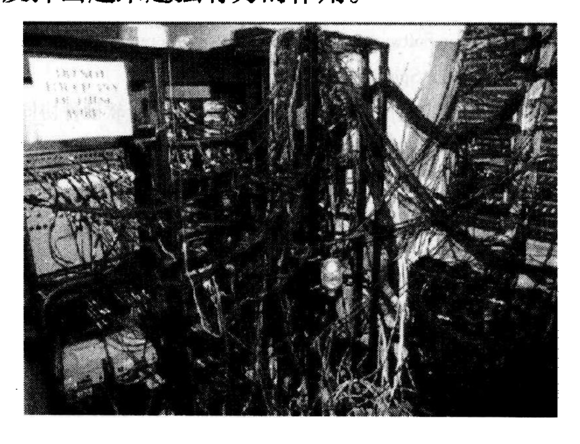


图3.1　可怕的有线网络

3.1　无线智能网络传感器构成

在大多数测控环境下,传感器采用有线方式使用,而在一些特殊的测控环境,如无人区、偏远地区和战场,使用有线电缆传输传感器信息则极为不便。为此,将智能网络传感器无线化是非常必要的。目前,无线智能网络传感器通常由5部分构成,即微处理器与存储模块、电源模块、传感器模块、执行器模块和无线通信模块。

3.1.1　微处理器与存储模块

微处理器模块是无线传感器节点的计算核心,标准的微控制器(可能具有DSP功能)、其他协同处理器和一些ASIC模块可以在满足一定能耗限制的前提下提供足够的处理能力。微控制器模块分为采样调理、数据处理、数据存储、通信接口和电源几部分,功能如下:

(1)模拟信号调理、滤波、放大、A/D 转换。

(2)数字信号暂存于缓存中,并对传感器采集的数据进行软件预处理。

(3)提供相应的接口与 RF 模块进行数据交换,负责链路管理与控制、执行基带通信协议和相关的处理过程,包括链接建立、频率选择、链路类型支持和媒体接入控制等。

目前的处理器还不完全具备智能传感器的应用需求,现有的节点方案中,基本上是在现有处理器/控制器中做出的最优与无奈的选择,这必然丧失了理想中无线智能网络传感器的部分功能。由于所有的控制、任务调度、能量计算、功能协调、通信协议、数据整合和数据存储都在微控制器模块支持下完成,所以,处理器的选择在无线智能网络传感器设计中是至关重要的。

在存储方面,根据整个传感器网络的结构,各节点存储的快速性、易失性需求有很大差异。例如,在一个网络体系结构中,若所有信息需要立即送往汇集节点(或 Sink 节点),则对节点存储空间的需求很小;但若目标是为了使通信总量最小化,需要在各节点中进行大部分运算,则对节点存储空间有很高要求。节点存储器设计主要是依据无线传感器网络的应用需求而定。

由于闪存在造价和存储能力上的突出表现,它是节点数据存储的首选。但由于在同一物理位置的可重复读写次数太少,闪存的应用受到了一定限制。另外,还可以采用磁性随机存储器(Magneto Resistive Random Access Memory, MRAM)进行存储。值得注意的是,半导体和硬盘存储能力的增长速度超过了摩尔定律的预计。在无线网络传感器中应用非易失性存储器至少面临两个方面的挑战:一是节约能量;二是适应较短的、仅包括几个单字节的数据处理存储能力。由于网络控制和传感器数据中很大一部分具有较低的信息熵,因此还需要采用压缩技术减少所需存储和传输的数据量。

在低功耗方面,传感器节点使用的处理器应功耗低,且支持掉电模式。处理器功耗主要由工作电压、运行时钟、内部逻辑复杂度以及制作工艺决定。工作电压越高、运行时钟越快,其功耗也越大。掉电模式直接关系到节点的生命周期的长短。根据现在的电池技术的发展水平,要使节点在正常工作状态下保持长时间工作是很困难的。目前,使用 5 号电池供给 MCU 的无线传感器节点,满负荷工作只能持续十几个小时。为了让这样的系统工作一年的时间,系统需要在绝大多数时间内处在待机或者睡眠状态。这就要求处理器必须支持超低功耗的睡眠状态。随着低功耗电路和系统设计技术的提高,目前,已经开发出很多超低功耗微处理器。除了降低处理器的绝对功耗以外,现代处理器还支持模块化供电和动态频率调节功能。

在一个器件中,功耗通常用电流消耗来表示。器件消耗的电流与器件特性之间的关系为

$$I_{cc} = C\int V\mathrm{d}V \approx \Delta VCf \tag{3.1}$$

式中:I_{cc}为器件消耗的电流;ΔV 为电压变化的幅值;C 为器件电容和输出容性负载的大小;f 为器件运行频率。

从式(3.1)可以得到降低系统功耗的理论依据。将器件供电电压从 5V 降低至 3V,可以至少降低 40% 的功耗。降低器件的工作频率,也能成比例地降低功耗。因此,处理器模块的设计应遵循以下原则:

(1)选用尽量简单的 MCU 内核。首先,考虑系统对处理能力的需求;其次,再考虑功

耗问题。选择“够用就好”的带 Flash 的 8 位或 16 位内核的 MCU,简单的 MCU 内核功耗低,带 Flash 的 MCU 可将功耗降低 5 倍,既缩小了线路板的空间,又降低了成本。

(2)外围器件的合理使用。由于外围器件的使用不是很频繁,所以要选择带片选功能的外围器件,不使用它们时进入低功耗模式。减少外围器件的使用是节点降低功耗、减小体积的积极办法,但这要视系统可行性而定,并需要软件配合。

(3)选择低电压供电的系统。降低 MCU 的供电电压可以有效地降低其功耗。本文中采用 MCU 从与 TTL 兼容的 3.0V ~ 3.3V 供电。低电压供电可以大大降低系统的工作电流,从式(3.1)还可以看到,降低 MCU 的供电电压能够成比例地降低功耗。基于漏电流的考虑,选择 3V 供电电压要比 5V 供电电压的功耗下降 50% 。随着低电压 MCU 的选择,其他部分也要选择低电压的型号。

(4)选择合适的时钟方案。时钟的选择对于系统功耗相当敏感。一是系统总线频率应当尽量低。MCU 内部的总电流消耗可分为两部分运行电流和漏电流。运行电流几乎是和 MCU 的时钟频率成正比的,因此尽量降低系统时钟的运行频率可以有效地降低系统功耗。二是时钟方案,也就是是否使用锁相环、使用外部晶振还是内部晶振。但片内晶振的精度不高(误差一般在 25% 左右,即使校准之后也可能有 2% 的相对误差),而且会增加系统的功耗。

晶振频率是决定功耗的基本环节,从式(3.1)可以看出,工作电流与晶振频率成严格的线性关系,空闲、掉电模式的电流也有类似的线性关系。因此,尽可能地降低晶振频率能够有效地降低整机电流;但是,降低晶振频率往往会受到系统运行速度的制约,需要综合考虑各部分的工作速度和整机信息运算的速度,选择一个合适的最小晶振频率。MCU 的选型比较如表 3.1 所列。

表 3.1　主要微控制器性能比较

指标		微控制器			
		MSP430F147 (TI)	ADμC834 (Analog Device)	ATMeg128L (Atmel)	LPC2210 (Philips)
位宽/bit		16	8	8	32
主频/MHz		8	16	8	60
Flash/KB		60	62	128	—
EEPROM/KB		256B	62	4	—
Flash/EE Data Memory/KB		—	4	4	—
SRAM/KB		2	2.3	1	16
ADC		8 路 12 位	3 路 16 位 2 路 24 位	8 路 10 位	8 路 10 位
I/O		6 个 8 位	4 个 8 位	8 个 8 位	76
工作电压/V		1.8 ~ 3.6	3.0 ~ 5.0	2.7 ~ 5.5	3.0 ~ 3.6
电流/mA	工作	400μA	10	10	30
	空闲	1.6μA	4	5	—
	掉电	0.1μA	14μA	2μA	10μA

3.1.2 电源模块

能量问题是传感器网络节点面临的一个主要约束。目前面世的智能节点依靠电池只能连续运行几个小时至十几个小时。理论上,能量供应问题可以从两个不同方面来解决:第一种方法是在每个节点上安装能量源,如采用高能量的电池作为能量源。由于燃料电池能提供高密度的清洁能源,因此可以考虑将燃料电池应用在网络节点上,但以目前的硬件条件还无法在传感器网络节点中应用。第二种方法是从环境中采集能量。除了被广泛地应用于各种移动环境中的太阳能电池外,电磁能、声波、地震波、风能发电等其他能量方式也可用于电能转换。表 3.2 所列为目前主要电池的性能参数。

表 3.2　目前主要电池的性能参数

电池类型	铅酸	镍镉	镍氢	锂离子	聚合物	锂锰	银锌
重量能量比/W·h·kg⁻¹	35	41	50~80	120~160	140~180	330	—
体积能量比/W·h·L⁻¹	80	120	100~200	200~280	>320	550	1150
循环寿命/次	300	500	800	1000	1000	1	1
工作温度/℃	-20~60	20~60	20~60	0~60	0~60	-20~60	20~60
记忆效应	无	有	小	很小	无	无	无
内阻/mΩ	30~80	7~19	18~35	80~100	80~100	—	—
毒性	有	有	轻毒	轻毒	无	无	有
可否充电	可	可	可	可	可	否	否
价格	低	低	中	高	最高	高	中

3.1.3 传感器模块

智能网络传感器的感知部分是当前的技术瓶颈之一,这些技术不像半导体技术那样发展迅速。从功能应用和物理实现角度,传感器的限制比处理器或存储器更严格。例如,当计算和通信模块完成对环境的控制后,传感器与实际物理世界的接口技术成为一个重要的瓶颈问题。换能器是无线网络传感器的前端组件,它可以将一种形式的能量转换成另一种形式的能量。换能器的设计是网络体系结构中的一个重要问题。此外,传感器具有 4 个其他的组件:模拟组件、A/D、数字组件和微控制器。仅包含转换器的结构是最简单的,但当前技术趋势是在传感器网络节点中加入更多智能组件,同时重要的处理和计算能力也已经加入到网络节点中。

传感器网络的一个主要挑战是选择传感器的类型和数量,并确定传感器位置。由于不同传感器具有不同特性(包括解决方案、花费、精度、尺寸和能耗),所以传感器的选择也是一个难题。另外,还需要保证多种传感器的正常运行,融合来自不同传感器的数据。

另一个挑战来自于传感器类型及其应用方式的选择。较困难的问题在于传感器的相互影响。如采用声波传感器测量距离时,声音传输速度很大程度上依赖于温度和湿度,因此,考虑这两个因素才能提高距离测量的准确性。与传感器相关的其他几个设计任务包括容错性、错误控制、校准和时序同步。

3.1.4　无线通信模块

无线网络传感器节点之间、节点与基站之间通过无线信道收发数据。由于无线信道本身的特点，它所能提供的网络带宽相对于有线信道要低得多，目前，无线网络传感器采用的传输媒体主要有电磁波、红外线、可见光等，对电磁波和红外线介绍如下：

(1)电磁波。采用电磁波作为无线局域网的传输介质是目前应用最多的，主要是因为电磁波的覆盖范围较广，应用较广泛。使用扩频方式通信时，特别是直接序列扩频调制方法因发射功率自然的背景噪声，具有很强的抗干扰、抗噪声、抗衰落能力。一方面使通信非常安全，基本避免了通信信号的偷听和窃取，具有很高的可用性。另一方面，无线局域使用的频段主要是工业科学医疗频段(Industrial Scientific and Medical, ISM)，如433MHz、915 MHz、2.4GHz 等，且不会对人体造成伤害。所以，电磁波成为无线传感器网络可用的无线传输媒体。

(2)红外线。采用小于 1mm 波长的红外线作为传输媒体，有较强的方向性，由于采用低于可见光的部分频谱作为传输介质，使用不受无线电管理部门的限制。红外信号要求视距传输，窃听困难，对邻近区域的类似系统也不会产生干扰。但背景噪声高，受日光、环境照明等影响大，是目前 100Mb/s 以上，性能价格比高的网络唯一可行的选择。但它不适合传感器网络。

常用的物理介质为电磁波，基于电磁波的主流无线通信技术有蓝牙(Bluetooth IEEE 802.15.1)、射频(Radio Frequency, RF)、Wi-Fi(IEEE 802.11b)、Zigbee(IEEE802.15.4)、超宽带(Ultra Wideband, UWB)、红外线数据协会(Infrared Data Association, IrDA)。业界广泛建议传感器网络采用 915MHz ISM 频段。几种无线传输方式的比较如表 3.3 所列。

表 3.3　无线传输方式的比较

参 数	Bluetooth	802.11b	RF	ZigBee	UWB	IrDA
系统开销/K	60～250 较大	1M 大	2～4 小	4～32 小	小	小
电池寿命	较短	短	较长	最长	很长	长
网络节点	7	32	255	255～65000	-	2
传输范围/m	1～10	1～100	10～200	4～100	5～10	定向 1～3
传输速率/Mb/s	最大 1	最大 11	20kb/s～115kb/s	20kb/s～250kb/s	最大 1Gb/s	最大 16
频道带宽/MHz	79	80	50	80	7.5GHz	—
典型功率/mW	1	50	60	60	0.2	—
传输协议	窄带发射频谱	直接顺次发射频谱	跳频发射频谱	直接序列扩频频谱	窄脉冲发射频谱	4PPM

因为数据传输能量占能耗的主要部分，所以短距离无线通信组件很重要。在无线通信组件的设计和选择过程中，必须考虑以下 3 个层次的问题：物理层、MAC 层和网络层。提高无线通信组件的能耗和带宽效率是无线传感器网络研究中最主要的研究任务。无线通信组件的体系结构是网络结构体系和协议的重要组成部分，由于无线通信占了整个无

线传感器网络能耗主要部分，尤其是信道的监听花费很大，因此，对无线收发系统的能耗管理非常重要，最主要的问题是平衡传输能耗和接收能耗。通过采取以下措施减少通信模块的能量损耗。

1. 减少通信流量

通过减少通信模块发送和接收的比特数，能降低通信模块的能耗，减少通信流量的方法有以下几种：

(1)本地计算和数据融合。对传感器节点采集的原始数据和各个节点汇集的相关数据进行处理，发送有用信息，可以有效减少通信量。

(2)减少冲突。如果两帧同时发送，它们会相互重叠，结果导致接收到的信号难以辨认，需要重传才能把信息正确发送到目的地。冲突引起的重传造成很大的能量浪费，减少冲突可以有效节约能量。

(3)增加错误检测和校正机制。增加错误检测可以尽早发现错误，校正机制可以校正少量比特错误的数据包。错误检测和校正机制可以在给定误码率(Bit Error Rate, BER)的条件下有效减少数据包的重传，从而降低能耗。

(4)减少控制包的开销和包头长度。网络协议需要控制包和包头来维护其正常运行，但控制包和包头并不是用户所需的数据，应尽量减少控制包的数量，减小包头长度，从而降低能耗。

2. 增加休眠时间

无线通信模块存在发送、接收、空闲和睡眠 4 种状态。无线通信模块在空闲状态一直监听无线信道的使用情况，检查是否有数据发送给自己，而在睡眠状态则关闭通信模块。从 Deborah Estrin 描述的图 3.2 中可以看到：无线通信模块在发送状态的能量消耗最大，而在空闲状态和接收状态的能量消耗接近，略少于发送状态的能量消耗，在睡眠状态的能量消耗最少。如何让网络通信更有效率，减少不必要的转发和接收，不需要通信时，尽快进入睡眠状态是传感器网络协议设计需要重点考虑的问题。

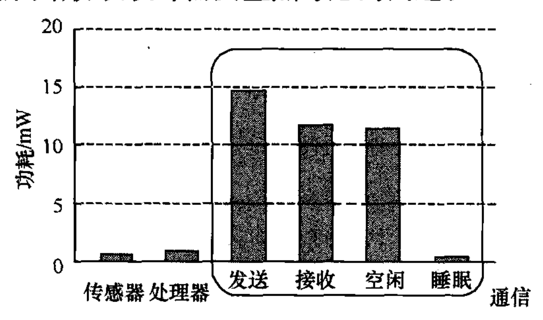


图 3.2　网络节点各模块的能量消耗示意图

3. 采用短距离多跳无线通信方式

简单而言，无线通信消耗能量 E_{wir} 与通信距离 d_{wir} 的关系为 $E_{wir}=k_{wir}d_{wir}$，其中，参数 k_{wir} 满足 $2<k_{wir}<4$。k_{wir} 的取值与很多因素有关，例如，传感节点部署贴近地面时，障碍物干扰源多，k_{wir} 的取值就越大；无线信道质量对信号发射质量的影响也很大。考虑诸多因素，通常取 k_{wir} 为 3，即通信能耗与距离的 3 次方成正比。随着通信距离的增加，能耗将急剧增加。因此，在满足通信速率的前提下，应该尽量减少单跳通信距离。一般而言，传感

节点的通信半径在 100m 以内比较合适。在无线传感器网络中，目前应用最多的是 Zigbee 和普通 RF 射频芯片，常见无线收发芯片的主要指标如表 3.4 所列。

表 3.4　可用于无线网络传感器的常见无线收发芯片主要指标

指 标	TR1000	nRF401 /Nordic	nRF905 /Nordic	RF2401 /RFMD	MC13192 /Zigbee	CC1010 /TI – Chipcon	CC2420 /TI – Chipcon	9Xstream /RFMD
频率/MHz	915	433/434	433/868/915	2.4 GHz	2.4GHz	402 ~ 904	2.4GHz	902 ~ 928
调制方式	OOK/ FSK	FSK	GFSK	GFSK	O – QPSK (DSSS)	GFSK	O – QPSK (DSSS)	FHSS
电源电压/V	2.7 ~ 3.5	2.7 ~ 5.25	1.9 ~ 3.6	1.9 ~ 3.6	2.0 ~ 3.4	2.7 ~ 3.6	2.1 ~ 3.6	7 ~ 18
发射电流/mA	12	9/5dBm	30/10dBm	10/ – 5dBm	30	11.9	17.4	200
接收电流/mA	1.8	10	12.5	15	37	19.9	19.7	70
睡眠电流/μA	5	8	2.5	1	2.5mA	0.2	1mA	26
接收灵敏度 /dBm	– 106	– 100	– 105	– 90	– 92	– 118	– 94	– 110
最大输出功率/dBm	+ 1.5	+ 10	+ 10	– 20 ~ 0	0	– 20 ~ 10	输出功率编程可控	+ 16 ~ + 20
数据速率 /(Kb/s)	115	20	100	1000	250	153.6	250	20
启动时间/ms	200	5	5	< 200	25	160	< 192	< 200
外围元件数目	17	10	20	2	20	4 ~ 6	12	< 30

3.2　无线智能网络传感器实例

3.2.1　智能灰尘

智能灰尘（Smart Dust）是美国 DARPA/MTO MEMS 支持的研究项目，其目的是结合 MEMS 技术和集成电路技术，研制体积不超过 $1mm^3$，使用太阳能电池，具有光通信能力的自治传感器节点，在战场上抛撒数千个微小的无线传感器节点，用于监控敌人的活动情况，而不让敌方察觉。通过自组织一个无线传感器网络，智能灰尘将对相关原始数据进行过滤，把重要的信息发送给中央司令部。Smart Dust 是一个具有电脑功能的超微型传感器，它由微处理器、无线电收发装置和使它们能够组成一个无线网络的软件组成。将一些灰尘散放在一定范围内，它们就能够相互定位，收集数据并向基站传递信息。由于体积小、重量轻、功耗低、自组织，该节点可以附着在其他物体上，甚至在空气中浮动。图 3.3 为智能灰尘较为形象的生成示意图。

近年来，由于硅片技术和生产工艺的突飞猛进，集成传感器、计算电路、双向无线通信模块和供电模块的微尘器件的体积已经缩小到了沙粒般大小，但它却包含了从信息收集、信息处理到信息发送所必需的全部部件。未来的智能灰尘甚至可以悬浮在空中几个小

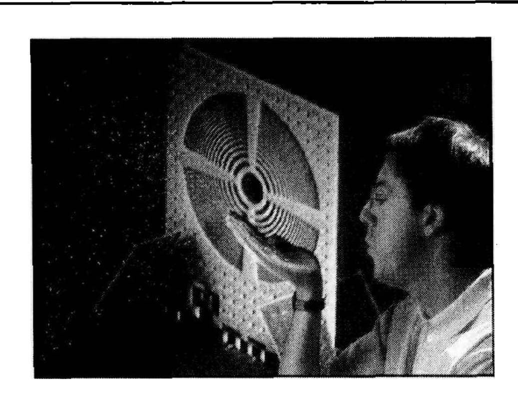


图 3.3　智能灰尘较为形象的示意图

时，搜集、处理、发射信息，它能够仅依靠微型电池工作多年，智能灰尘的远程传感器芯片能够跟踪敌人的军事行动，可以把大量智能尘埃装在宣传品、子弹或炮弹中，在目标地点撒落下去，形成严密的监视网络，敌方的军事力量和人员、物资的流动自然一清二楚。

智能灰尘系统结构如图 3.4 所列，实物及对比如图 3.5 所列。

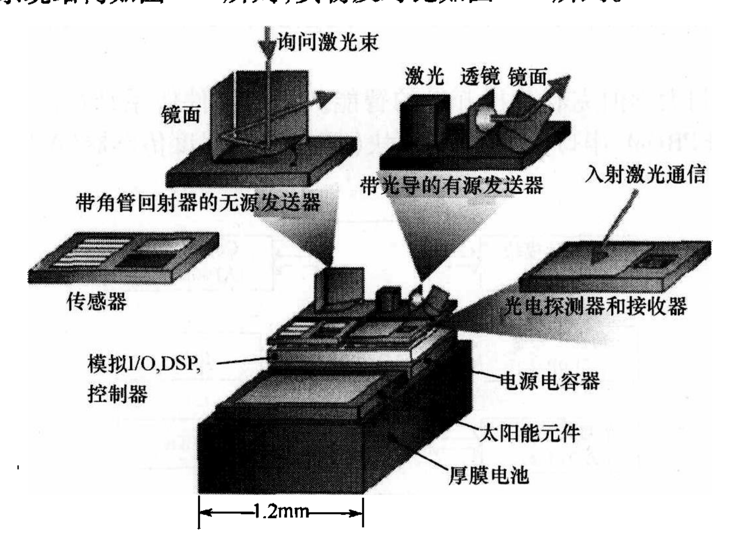


图 3.4　Smart Dust 系统结构图

智能灰尘的主要特点如下：

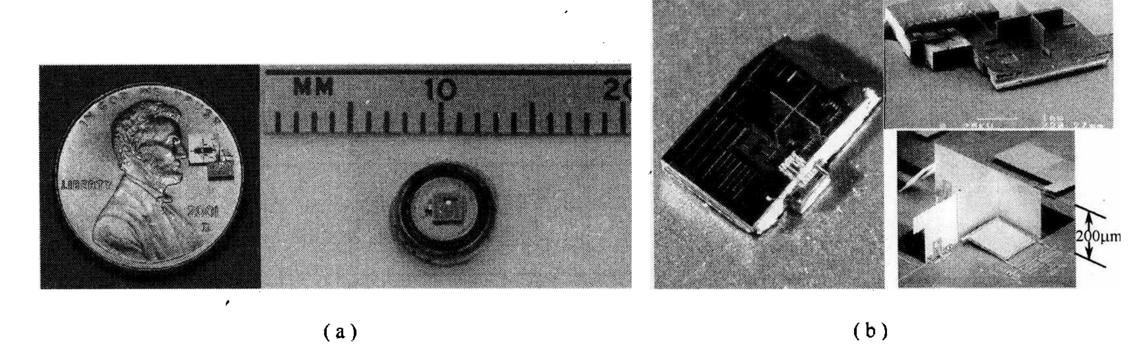
(1)采用 MEMS 技术，体积微小，整个传感器节点可以控制在 $1mm^3$ 左右。

(2)使用太阳能作为其工作能量的来源，具有长期工作的能力。

(3)采用光通信方式。一方面功耗比无线电小(如果采用被动光反射技术，则耗能更小)；另一方面不需要很长的天线，在体积上也可以做得非常小。另外，通信信道空分复用，所以基站可以同时与多个节点通信。

(4)光通信方式虽然降低了节点功耗，但其传输的方向性、无视距阻碍的要求给节点的部署带来很大挑战。

智能灰尘有被动和主动两种通信模式。被动模式中节点本身不发光，而是通过反射来自基站收发器(Base Station Transceiver, BTS)的光完成信息传递，这简化了节点复杂度，而且降低了节点功耗，不能主动发送消息，只能等待主站查询，所以响应速度比较慢。



(a)　　　　　　　　　　(b)

图 3.5　Smart Dust 实物及其对比图

主动模式在节点上增加激光、校准透镜和光束调节微镜等装置，在有数据需要发送的时候可以主动向周围的节点或者主站发送，这种方式增加了节点功耗，但减少了响应延迟。被动方式的传感器节点依赖基站完成通信，只能构建节点直接与基站通信的集中式网络；主动方式在解决多方向激光发射方面也有困难，这些技术的难点在一定程度上限制了智能灰尘的应用。

图 3.6 是加州大学伯克利分校开发的智能灰尘的硬件体系结构。它集成了处理器(AT90LS8535)、EPROM、串口、无线通信模块(TR1000)、温度传感器(AD7418)、光强传感器(CL9P4L)等。

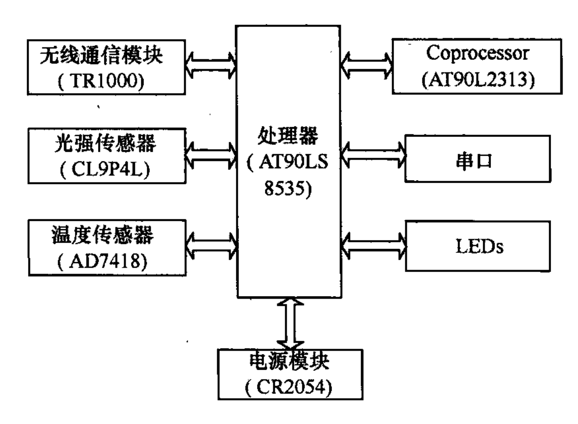


图 3.6　智能灰尘的硬件体系结构框图

因为系统是由电池供电，所以能耗受限。为了减少功耗，各个硬件均采用小体积、低功耗的器件。为了实现系统的微型化，硬件电路采用模块化设计，由主机模块、传感器模块、通信模块、电源模块 4 部分组成。

(1)主机模块。微处理器采用 Atmel 公司的 AT90LS8535。AT90LS8535 是 8 位 AVR 单片机，内嵌 8KB 内存用于存储程序代码，还有 512B 的 RAM 用于存储数据；外接 4MHz 晶振，保证较低功耗。副处理器的主要功能是存储临时数据。

(2)传感器模块。光强传感器采用 Clairex 公司的 CL9P4L，它实际上就是一个光电二极管，能将光强的变化转化为电阻的变化；温度传感器采用 AD 公司的 AD7418。

(3)通信模块。无线收发器件采用 RFM 公司的 TR1000。TR1000 外围电路简单，具

有睡眠模式以降低功耗，可达到115.2Kb/s的数据传输速率，理想传输环境下有效通信距离为1000m。

(4)电源模块。电池采用Panasonic公司的CR2054。CR2054储存了560mAh的电能，并且体积较小。传感器系统处于收发数据的工作模式下可以连续供电35h，而处于休眠状态等节能模式下能够供电至少1年。

3.2.2 Mica系列节点

Mica系列节点[1,2]是由UC Berkeley大学研制，由Crossbow公司生产的无线传感器节点。图3.7为其组网示意图。图3.8列出了3类Mica节点，包括传感器和数据采集、处理和无线通信、网关和网络接口。每个Mica节点由不同的Mica设备组成。

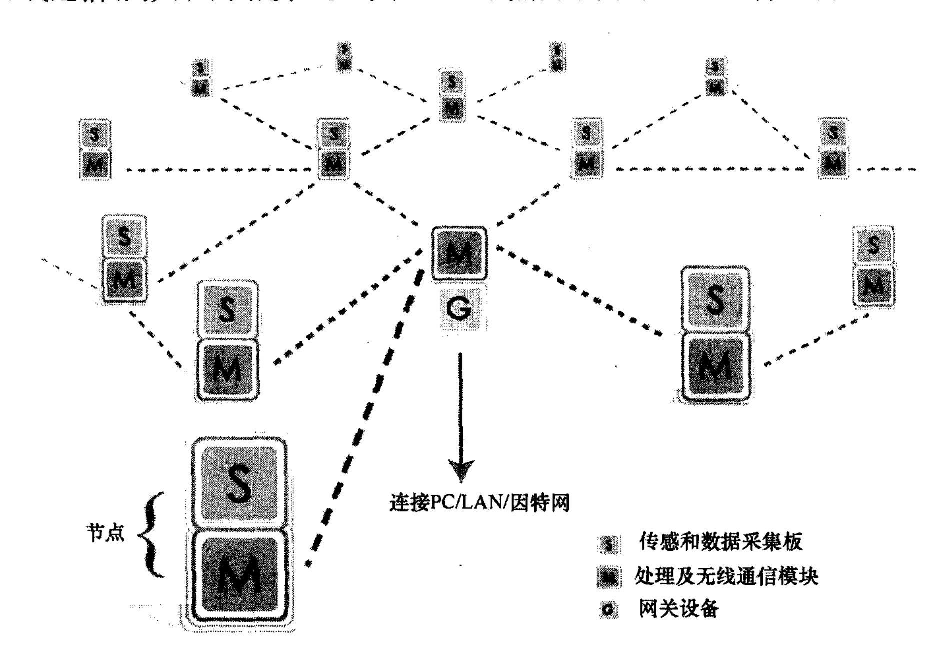


图3.7　Mica系列节点的组网示意图

目前应用最广泛的是Mica、Mica2和Micaz尘埃节点。Mica系列节点包含一个Atmel公司的ATmega128L微控制器，它包含8位RISC(精简指令集计算机)、128KB闪存、4KB SRAM和最高达1MIPS/MHz的带宽，Mica和Mica2的CPU时钟频率分别为4MHz和7.37MHz。Mica2和MicaDOT采用CC1000芯片，实物如图3.9和图3.10所列。

Mica和Mica2的连接器用于连接具有多种传感器的附加板。目前支持的传感器包括光、温度、湿度、压力、红外线、声音、加速度计、磁力计、风速计和风向针等。同样支持简单的执行部件，如彩色LED和蜂鸣器。

Mica3的无线模块使用的是Chipcon公司的CC1020。该芯片使用了GFSK的编码调制方式，拥有6Kb/s的数据吞吐量，输出功率达到27dBm，可以传送更远的距离，更适合于室外应用；Micaz则使用了Chipcon公司的CC2420。CC2420是较早支持Zigbee通信技术的通信芯片，载波频率为2.4GHz，数据传输率最高可达250Kb/s，通信距离为60m~150m，更适合于室内应用。除了通信技术不同以外，两款节点其他设计与Mica2都是相同的。

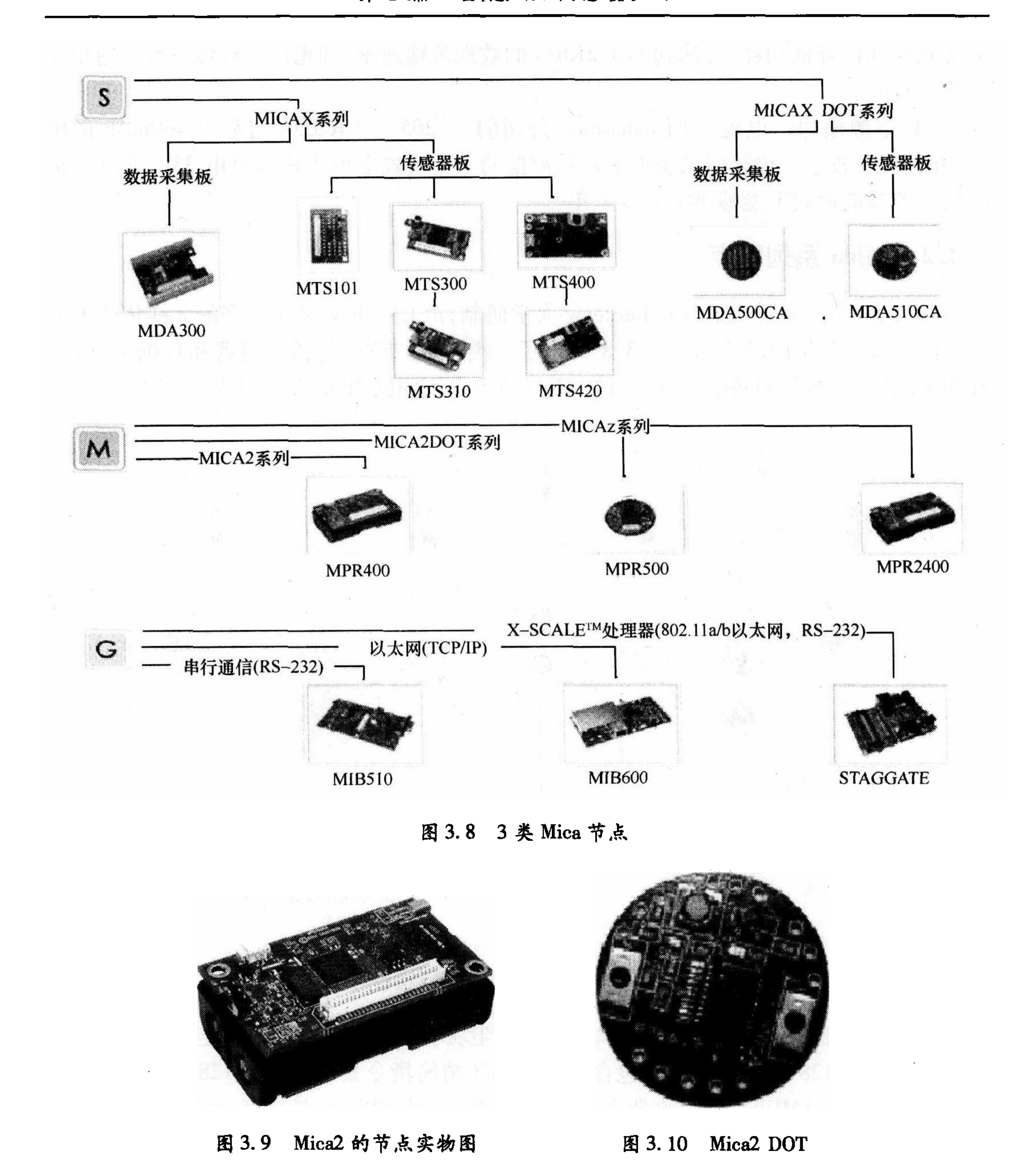


图 3.8　3 类 Mica 节点

图 3.9　Mica2 的节点实物图

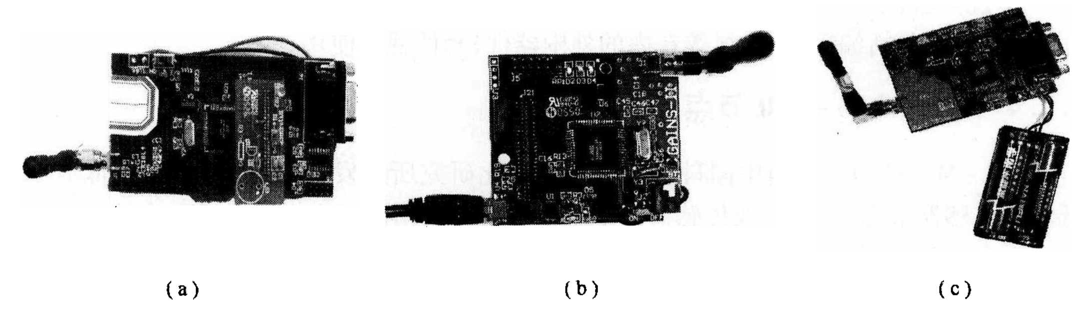
图 3.10　Mica2 DOT

3.2.3　GAINS 节点

中国科学院计算所宁波分所在无线传感器网络和低功耗设计方面经过多年研究，开发出了多种无线传感器网络节点产品，包括 GAINS 系列节点[3]、专业低功耗处理器WO-LPP、事件驱动的无线传感器网络操作系统 GOS 等。

GAINS-1 节点兼容同类 GAINS 节点的所有功能，节点的设计都是以无线通信为中心，并在数据采集、数据处理、微型化和低功耗等性能方面有很大提高。GAINS-2、GAINS-3 及 GAINSU 节点在 GAINS-1 基础上做了改进，分别提供了不同的传感器及各

种接口,为无线传感器网络的研究带来了方便。GAINZ 是在 GAINS 基础上实现了对 2.4GHz IEEE802.15.4/Zigbee 标准的支持,如图 3.11 所列。



(a)　　(b)　　(c)

图 3.11　GAINS 节点原型
(a)GAINS-3;(b)GAINSU;(c)GAINZ。

miniGAINS 系列节点采用纽扣电池供电,通过外扩的编程板对节点进行配置。板上接口丰富,包括 JTAG 接口、USB 接口、外部供电接口等。JTAG 接口实现对节点的仿真和编程,通过 JTAG 接口进行仿真和编程;USB 接口实现与 PC 机通信并对节点供电;外部供电接口支持 9V~11V 直流电源供电。

miniGAINS 是在 GAINS 节点的基础上将功能、功耗和体积变得更为简洁的产品。它采用低功耗微处理器芯片 ATmega128,射频部分采用 CHIPCON 公司的 CC1000 芯片,整个系统分为处理器模块、供电模块和射频模块,其中处理器模块和供电模块在同一个板上,射频模块单独一个板,并通过特殊的接口将两者上下连接在一起,同时处理器模块集成了传感器功能,供电模块采用高质量的纽扣电池供电,从而大大缩小了模块的体积。同时与之配套的编程调试板可为 miniGAINS 提供标准的 JITG 接口,并可连接 USB 和外接直流电源,方便客户调试和二次开发。在外包装上 miniGAINS 采用铝合金外盒,轻巧美观,如图 3.12 所列。

软件上 miniGAINS 全面兼容 GAINS3-433 开发套件,提供了面向无线传感器网络的 MAC 协议堆栈及面向应用层设计的接口(有库文件和源代码两种形式)。现阶段,由于这方面的协议还没有统一的标准,主要是提供了一个透明的输入输出流控制,以及一些基本的 MAC 层的控制,并且提供了丰富的对外接口便于用户开发自己的协议。在此基础上用户可以构建自己的系统,组成更复杂的网络。



图 3.12　Mini Gains 节点实物图

miniGAINS 主要特性如下:

(1)提供集成电路及其外围器件的参考设计。

(2)配套的编程调试板提供标准的 JITG 接口和 USB 接口,用于在线硬件调试。

(3)功能丰富、接口清晰的协议栈工作频段为 433MHz,全面兼容 GAINS3 模块软件。

(4)网络可视化后台软件。

(5)纽扣电池供电,小巧简便。

(6)板子封装尺寸仅为 4.85cm×3cm。

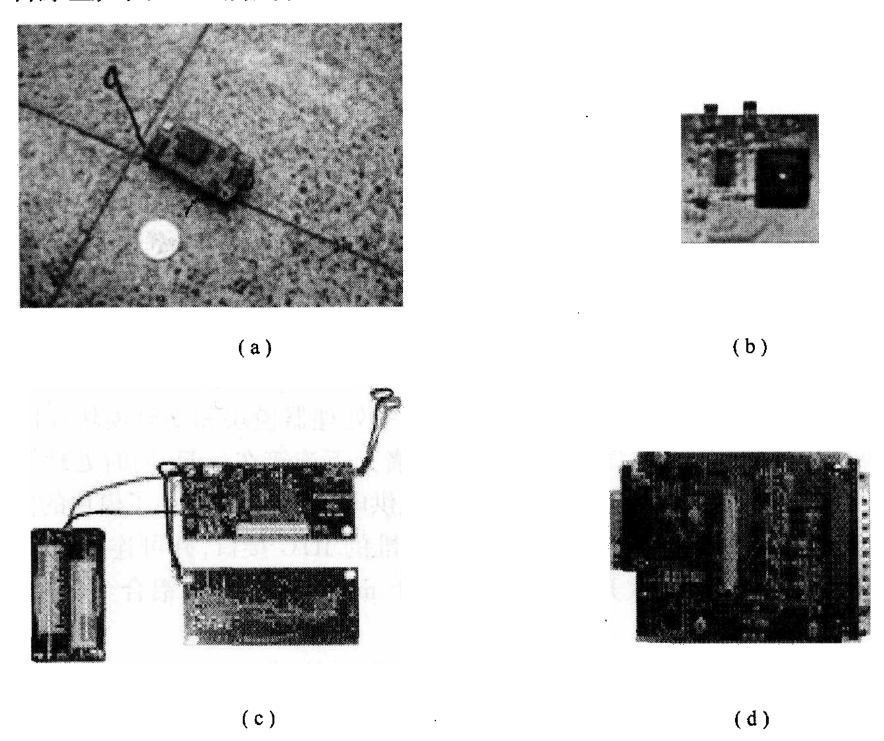
(7)采用的元器件大都为低功耗器件,在睡眠状态,电流仅为 5mA,发射状态下为 9mA,在掉电节能模式下,电流更是只有 110μA 左右。

(8)协议栈使用 C 语言开发,易于开发与移植。

(9)提供包括编程器、天线等在内的外围器件,套件视频使用说明。

3.2.4 SIA - MS - 1.0 节点

SIA - MS - 1.0[4]是由中国科学院沈阳自动化研究所开发的是一种通用的、低成本、低功耗传感器节点,它为无线传感器网络通信协议和应用研究提供了灵活的实验平台,该硬件平台原型如图 3.13 所列。



(a)　(b)　(c)　(d)

图 3.13 SIA - MS - 1.0 硬件平台原型

SIA - MS - 1.0 无线传感器网络实验平台主要由数据处理子系统、数据采集子系统、无线通信子系统和电源子系统构成。其结构组成图如图 3.14 所列。

数据处理子系统由 Atmel 公司的 8 位 AVR - ATmega128L 微控制器、AT45DB04 存储器、嵌入式操作系 TinyOS、Chipcon 公司的 CC1000 超低功耗的无线射频收发单元及 JTAG&UART 接口构成,主要用于数据处理与无线通信。SIA - MS - 1.0 传感器模块由麦克风、声响器、光传感器、温度传感器、两轴加速度传感器、两轴磁力传感器及辅助电路组成,用于感知对外部环境参数。

传感器板通过 51 针外扩连接器与通信及处理器子系统连接。SIA - MS - 1.0 程序下载模块由包括一个 RS232 串行接口、一个用于程序下载的并行接口(打印并口)、JTAG 接口、51 针外扩连接器及 DC - DC 转换单元,用于程序下载与调试。电源子系统负责给 SIA - MS - 1.0 供电。

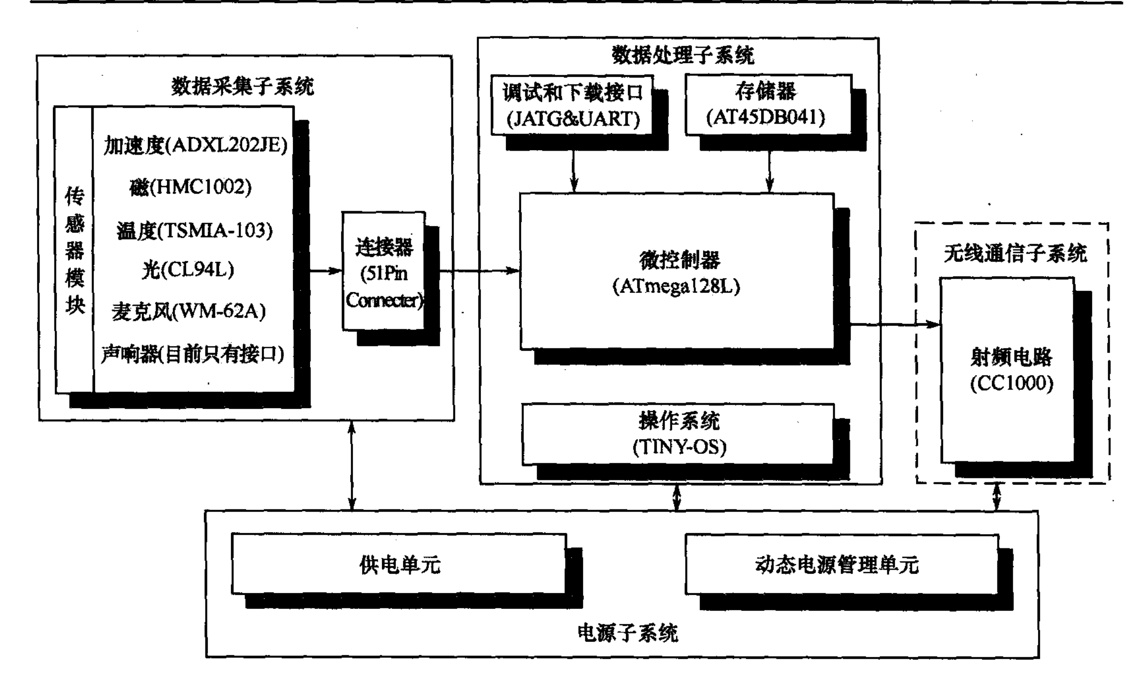


图 3.14　SIA－MS－1.0 的系统结构

3.2.5　WMNMCS[5,6]

空军工程大学无线传感器网络研究室于 2004 年开始研究无线传感器网络的相关技术，主要包括节点硬软件平台、MAC 协议、路由协议、节点数据融合、网络数据聚集、无线传感器网络与因特网互联技术、网络模拟器等。在传感器网络节点方面，目前已经研制出具有自主知识产权的三代节点系统：WMNMCS－Ⅰ、WMNMCS－Ⅱ和 WMNMCS－Ⅲ。

WMNMCS 模块的所有器件都集成在 4cm×4cm 的印刷电路板上（二次集成后仅有一元硬币大小），面向低端，采用 MCS－51 微处理器；面向高端，微处理器采用 ARM 微控制器。系统软件采用嵌入式实时操作系统；B/S 模式的通信，网络协议遵循工业标准协议支持 TCP/IP(4.0 版本)、HTTP 和 PPP/SLIP、UIP9.0；网络接口有 RS232、以太网和 CAN。WMNMCS 模块具有多功能、体积小、低功耗、高可靠性等诸多优点。图 3.15 为 WMNMCS 节点实物图。

WMNMCS 智能网络传感器适用范围广泛，在军用和民用领域都有广泛的应用前景。典型应用包括以下几方面：

(1)实现远程设备故障诊断。

(2)无固定基础设施的远程数据采集。

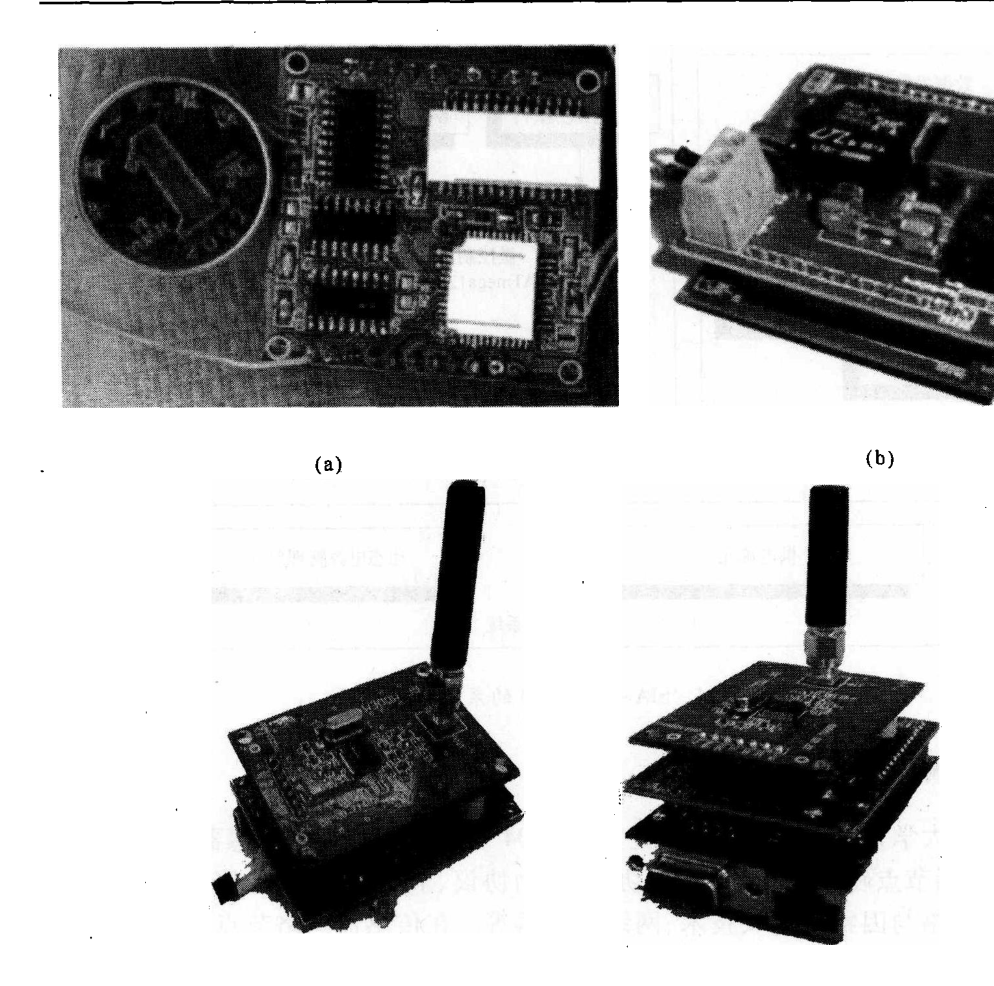
(3)野外、厂矿等环境比较恶劣的场合。

(4)没有固定工作环境的场合。

(5)对人体有害的场合。

(6)一些对体积和重量有严格限制，但需要远程测控的设备或现场。

关于 WMNMCS 的更多内容，请参见本书第 15 章。



(a)　(b)

(c)

图 3.15　WMNMCS 节点实物示意图

(a) WMNMCS－Ⅰ；(b) WMNMCS－Ⅱ；(c) WMNMCS－Ⅲ。

此外，还有许多无线智能网络传感器节点，表 3.5 所列为目前较为知名和应用较为广泛的实例。

表 3.5　无线智能网络网络传感器实例

名 称	处 理 器	厂家	无线芯片	技术	电池类型	发布日期
WeC	AT90S8535	Atmel	TR1000	RF	Lithium	1998
Renee	ATmega163	Atmel	TR1000	RF	AA	1999
Mica	ATmega128L	Atmel	TR1000	RF	AA	2001
Mica2	ATmega128L	Atmel	CC1000	RF	AA	2002
Mica2Dot	ATmega128L	Atmel	CC1000	RF	Lithium	2002
Mica3	ATmega128L	Atmel	CC1020	RF	AA	2003
Micaz	ATmega128L	Atmel	CC2420	Zigbee	AA	2003
Toles	MSP430F149	TI	CC2420	Zigbee	AA	2004

（续）

名 称	处 理 器	厂家	无线芯片	技术	电池类型	发布日期
XYZnode	ML67Q500x	OKI	CC2420	Zigbee	Ni - Mn	2005
Platform1	PIC16LF877	Microchip	Bluetooth&RF	AA	2004	
Platform2	TMS320C55xx	TI	UWB		Lithium	2005
Platform3	ARM7TDMI + Bluetooth 集成			Zoove	Battery	2005
Zabranet	MSP430F149	TI	9Xstream	RF	Batteries	2004
SIA - MS - 1.0	ATmega128L	Atmel	CC1000	RF	AA	2005
WMNMCS - Ⅰ	P89V51	Philips	nRF905	RF	AAA	2005
WMNMCS - Ⅱ	ADuC832/834	AD	nRF905	RF	AAA	2006
WMNMCS - Ⅲ	LPC2210	Philips	CC2420	Zigbee	AAA	2007

3.3　无线智能网络传感器天线设计

在无线智能网络传感器系统中，天线是一个需要高度重视的元件，是用于接收或辐射电磁能量的设备。它可以看作是将电能变为电磁能形式的转化器，反之亦可。天线有两个基本的功能：接收天线截取电磁能并通过适当的电力设备将其转化为电能，发射天线通过电力设备将电信号转化为电磁能。

在满足低功耗和低成本两个基本设计准则下，绝大部分无线网络传感器按小型化设计，而这些要求使得天线的设计变得重要而且困难。此外，为了适应网络节点的外观设计要求而需要调整天线设计，这就更增添了难度。因此，通常将天线作为智能网络传感器系统中最后设计的一个电子元件。天线设计难易程度也取决于网络传感器节点工作的频率：较高频率上，物理尺寸很小的天线设计并不困难，如一个谐振在 2.4GHz 的半波偶极子天线只有 6.25mm 长；在相对较低频率上，设计小尺寸天线则比较困难，如 433MHz/434MHz，而此时天线在自由空间的工作波长要比天线实际的物理尺寸长的多。

传输天线是一个将电能转化为电磁辐射的转化器。若电磁辐射在各方向上都是均匀的，则这种天线就称为等方向性天线。一个等方向性天线是全向的，并在同一水平面上的各个方向上辐射相等的能量相反，方向性天线只在某一个或多个特定方向上辐射电磁能。若方向性天线只在一个方向上辐射电磁能，则是单向的；若它在两个方向上辐射，则是双向的。

3.3.1　天线类型选择

由于天线的形状、构造和材料不同，就会有许多不同类型的天线。RF 系统中常用细线的单极化天线。这种天线的运行原理与同轴电缆的原理相同。单极化天线有各种型号，包括宽带的、圆锥的、大尺度和小电力单极化天线。通常使用同轴传输线将信号输入到天线，电缆和天线之间的电阻匹配是由低频的集中参数感应电容电路和高频短截匹配电路完成。

鞭形天线可能是移动通信中应用得最为广泛的一种天线，其次可能是普通模式的螺

旋天线。鞭形天线与单极化天线相似,但鞭形天线是由活动杆制成的。鞭形天线在根本上是电容性天线或双导电天线,它由一个绝缘支架支撑并与其他结构隔绝,即是绝缘的。鞭形天线的长度通常是辐射电磁波波长的 1/10 或 1/5。

微带天线因其低调的外表和在印制电路上容易构成而较为流行。微带天线也可制作成各种形状和尺寸,同时还可以使用电解质作为构成材料,而这种电解质能够装在较小的空间内。它的缺点是有效性较低。

细线偶极天线是通信系统中最为常用的天线之一。同时还有原理相同而运行方式不同的其他天线,包括电小偶极天线、发偶极天线、折叠式单极化天线和旋转天线。除此之外,还有很多不同种类的天线,如八木式、同轴式、环形、螺旋形、对数周期式、隙式、凹口式、触角式、透镜式和反射器式天线。另外,每种类型的天线的形状和运行原理都不同。

天线也可排成阵列。阵列天线集中了各种天线阵元,如单极化、隙式、环状、微带等。两种常用于天线阵列中的是八木—宇田天线和对数周期天线。八木—宇田天线包括 3 个或更多半波阵元,1 个驱动,1 个反射,1 个或多个控制。八木—宇田天线提供高方向性和高增益。对数周期阵列是多阵元、单一方向、窄波束天线,它的电阻和辐射特性是激发频率的对数函数。这样的结果使对数周期阵列中阵元的长度和间隔从开始阵元到结束阵元都成对数地增加。对数周期天线常应用于宽带系统中。

阵列天线的另一类是平面或扇区天线,它们有多个阵元来辐射和接收来自同一小区内的不同扇区的信号。平面或扇区天线常常是平面状的且用塑料包裹,用于隔绝其他阵元或其他金属以及其他带电元件。

在频率低于 3GHz 的通信系统中,应用了许多不同类型的天线,包括单极化天线、偶极天线和阵列天线。碟形卫星天线常用于微波频段,即接近 3GHz 或更高的频率。

在无线智能网络传感器中,天线类型的选择主要取决于它的应用。由于便于携带且具有免受机械和外部环境损害等优点,内置天线通常作为首选。目前,无线网络传感器有如下几种内置天线可供使用:

(1)用电路板上的金属印制线作为天线。其优点是不必购买、加工或安装任何形式的元件到电路板,成本低,但会占用宝贵的电路板空间,因此也不是零成本。此外,该天线非常薄,这对于降低网络节点的体积来说是一个优点。此类天线的最大缺点是性能较差。尽管选用低电阻率的铜,由于其厚度太薄使得串联电阻相对较高,低品质的电路板材料也会增加介质损耗。在电路板上的走线,天线更容易与有耗元件、其他走线和噪声源发生耦合。并且印制天线的调谐误差将会很大,这是由电路板加工过程的蚀刻误差引起的。由于所需的蚀刻精度远远高于电路板上简单连接线的精度要求,因此,控制公差的成本将会很高。

(2)将简单的导线天线或金属条带天线作为元件安装在电路板上。因损耗很低且置于电路板上方,这类天线的性能比印制天线有明显提高,但由于置于电路板上方,所以极易和一些噪声源,如开关电源电路内的电感产生耦合。导线天线可以是偶极子天线,也可以是环型天线。对用在人体上的传感器,如健康监视器件,常采用环型天线。这类天线也称磁场天线,位于与人体垂直的平面内。导线天线需要介质材料(如塑料)支撑,从而使其机械外形及相应的谐振频率达到必要的容差要求。这种天线很难在自动装配线上进行安装,只能人工安装和焊接,不管怎样,导线天线是介于低成本、低效率的印制天线与相对

高成本、高效率的外置天线之间很好的折中形式。

(3)特殊的陶瓷天线元件。此类天线可以进行自动安装，尺寸比导线天线小，并且不需要调整。但价格比导线天线昂贵，且只在最常使用的频段使用，如915MHz和2.4GHz的工业、科学和医疗(ISM)频段。

外置天线通常没有内置天线那样的尺寸限制，距离网络节点中的噪声源也较远，因此具有很高的性能。对那些需要尽可能大的距离且必须选用定向天线的应用来说，外置天线几乎是必选的。当节点应用在大型家用电器中时，如电冰箱和其他一些大型家用电器，采用外置天线还可以免去采用金属外壳屏蔽的麻烦。虽然外置天线可提供相对较高的性能和设计的灵活性，但它们通常也比较昂贵，不仅需要购买天线，而且还需另购一些高质量的射频连接器(如法兰盘、射频导线等)。

此外，天线的频率选择性是一个常被忽视的问题。因为内嵌天线在节点设计者的控制之下，其选择性可融于收发器系统的设计之中。而在使用外置天线时，用户可能会更换一些选择性不明的天线。因此，在进行节点设计时，设计者需要包含额外的射频选择性，从而增加额外成本。

外置天线并不都是很昂贵的，例如，Ross[7]等人介绍了一种隐蔽安装在门把手里并用门把手作为天线的无线传感器网络节点。

3.3.2　天线特性

1. 天线方向性系数 D_{antenna}

天线方向性系数定义为最大辐射密度与向四周均匀辐射相同功率 P_{rad} 时的辐射密度之比，即

$$D_{\text{antenna}} = \frac{P_{\text{d,max}} 4\pi r^2}{P_{\text{rad}}} \tag{3.2}$$

式中：D_{antenna} 为天线方向系数，无量纲；$P_{\text{d,max}}$ 为某个方向上的最大辐射功率密度(W/m^2)；r 为从观察点到天线的射线距离(m)；P_{rad} 为天线总的辐射功率(W)。

考虑到工作环境对电磁波传播散射的影响，天线的最大辐射方向在无线传感器网络中通常没有多大意义，尤其当网络在室内工作时。在室外环境中，有些应用比较接近自由空间的传播条件(对入射波几乎没有散射)，因此可通过提高天线方向性系数来增加通信距离。对于网络节点设计者而言，天线效率要比天线方向性系数更重要。

2. 天线效率

天线效率定义为

$$\eta = \frac{P_{\text{rad}}}{P_{\text{accept}}} \tag{3.3}$$

式中：η 为天线效率(无量纲)；P_{accept} 为天线实际接收的功率(W)。

天线效率 η 只考虑天线的输入功率。

为了保证从发射机到天线的最大功率传输，天线阻抗必须正确，为此可定义阻抗失配因子(无量纲)为

$$M_{\text{imp}} = \frac{P_{\text{accept}}}{P_{\text{avail}}} = 1 - |s_{11}|^2 \tag{3.4}$$

式中：P_{avail}为匹配情况下天线能够获得的最大功率；s_{11}为与天线输入端反射系数有关的 s 参数。

忽略天线极化因素，天线增益 G 可定义为天线方向性系数、效率和失配因子三者的乘积，即

$$G = D_{antenna}\eta M_{imp} = \frac{P_{d,max}4\pi r^2}{P_{rad}}\frac{P_{rad}}{P_{accept}}\frac{P_{accept}}{P_{avail}} \tag{3.5}$$

如果设计不当，电小天线的工作效率会很低，即意味着由发射机送来的能量绝大部分将转化为热能而不是有效辐射，而根据互易理论，低效率天线接收到的绝大部分能量也不能送到接收机。根据戴文宁等效电路定理，天线效率可以表示为

$$\eta = \frac{R_{rad}}{R_{rad} + R_{loss}} \tag{3.6}$$

式中：R_{rad}为天线的辐射电阻（Ω）；R_{loss}为天线的损耗电阻（Ω）。

天线辐射电阻是在天线的馈电点处辐射功率与均方根电流的比值，即

$$R_{rad} = \frac{P_{rad}}{I_{fb}^2} \tag{3.7}$$

式中：P_{rad}为天线的辐射功率（W）；I_{fb}为天线馈电点的均方根电流（A）。

例如，电小偶极子的辐射电阻可表示为

$$R_{rad} = 80\left(\frac{L_{dip}}{\lambda}\right)^2 \tag{3.8}$$

式中：L_{dip}为偶极子长度（m）；λ 为自由空间工作波长（m）。

假设 $L_{dip} = 0.0125\text{m}$，$\lambda = 0.125\text{m}$（即工作频率为 2.4GHz），$L_{dip}/\lambda = 0.1$，则 $R_{rad} = 7.9\Omega$。电小尺寸天线的辐射电阻通常小于 1Ω，尤其在更低的工作频率上，相同的偶极子长度 $L_{dip} = 0.0125\text{m}$ 在 400MHz 辐射电阻只有 0.22Ω。

3.3.3　鞭状天线

天线是无线通信模块的重要组成部分，在满足低功耗和低成本设计原则下，如何设计工作效率较高的天线，必须从天线材质、形状、长度及工作频率几个技术指标加以考虑，尤其是天线的放置策略十分关键，如果设计不当，天线的工作效率会很低，发射端送来的能量绝大部分将转化为内耗（如热能）而不是有效辐射。根据应用环境与场合的不同，本节介绍两种天线设计类型：鞭状天线和 PCB 微带环形天线，均采取小型化设计。

根据麦克斯韦理论，在球坐标系中，在距离远大于无限小电流元的观察点处，无限小电流元辐射的电场和磁场为

$$E_r = -j\frac{Idl}{2\pi}e^{-jkr}Z_0k^2\left[\frac{j}{(kr)^2} + \frac{1}{(kr)^2}\right]\cos\theta \tag{3.9}$$

$$E_\theta = -j\frac{Idl}{4\pi}e^{-jkr}Z_0k^2\left[-\frac{1}{kr} + \frac{j}{(kr)^2} + \frac{1}{(kr)^3}\right]\sin\theta \tag{3.10}$$

$$H_\phi = j\frac{Idl}{4\pi}e^{-jkr}k^2\left[\frac{1}{kr} - \frac{j}{(kr)^2}\right]\sin\theta \tag{3.11}$$

式中：E_r 为沿 r 方向的电场分量（V/m）；E_θ 为沿 θ 方向的电场分量（V/m）；H_ϕ 为沿 ϕ 方向的电场分量（A/m）；I 为电流（A）；dl 为电流元的长度（m）；k 为波数，其值为 $2\pi/\lambda$（m^{-1}）；Z_0 为自由空间的波阻抗，约等于 376.73Ω；r 为观察点与电流元之间的距离，且 $r \gg dl$（m）。

在球坐标系中，无限小电流环的电场与磁场分量为

$$H_r = \frac{\kappa IA}{2\pi}\mathrm{e}^{-\mathrm{j}\kappa r}\kappa^2\left[\frac{\mathrm{j}}{(\kappa r)^2} + \frac{1}{(\kappa r)^3}\right]\cos\theta \tag{3.12}$$

$$H_\theta = \frac{\kappa IA}{4\pi}\mathrm{e}^{-\mathrm{j}\kappa r}\kappa^2\left[-\frac{1}{\kappa r} + \frac{\mathrm{j}}{(\kappa r)^2} + \frac{1}{(\kappa r)^3}\right]\sin\theta \tag{3.13}$$

$$E_\phi = Z_0\frac{\kappa IA}{2\pi}\mathrm{e}^{-\mathrm{j}\kappa r}\kappa^2\left[\frac{1}{\kappa r} - \frac{\mathrm{j}}{(\kappa r)^2}\right]\sin\theta \tag{3.14}$$

式中：$\kappa = \frac{2\pi}{\lambda}$；$r$ 为天线与电流环之间的距离；I 为电流；A 为电流环的面积；H_r 为 r 方向磁场分量；H_θ 为 θ 方向磁场分量；E_ϕ 为 ϕ 方向电场分量。

各等式中包含随 $\frac{1}{\kappa r}$ 变化的项，这些项代表可传播电磁波。当 $r < \frac{\lambda}{2\pi}$ 时，$\frac{1}{(\kappa r)^2}$ 和 $\frac{1}{(\kappa r)^3}$ 项的辐射比 $\frac{1}{\kappa r}$ 大得多，如果天线附近强电磁场存在损耗材料，原本可以辐射的能量将被消耗掉，对于小尺寸板级的天线设计这是一个很大的问题。

因此，高频设计中，一个重要的规则是在半径 $\frac{\lambda}{2\pi}$ 的范围内，避免放置损耗材料，具体如下：

（1）电源、传感器、元器件及其他具有高射频损耗的材料必须远离天线。

（2）电路板上印制电路走线尽管采用了低电阻率的铜材料，但由于走线非常细，仍具有较高的射频阻抗，因此，天线附近的走线必须尽量少。

（3）选择聚四氟乙烯材料的板基，并在表面镀银，以减少材料对辐射能量的消耗。

（4）根据实际设计经验，在天线 $\frac{\lambda}{100}$ 距离内不能布设表面贴元器件和印制板走线。因此，本文节点的各板级模块尺寸均为 4cm × 5cm。

3.3.4　PCB 微带环形天线

微带天线是在带有导体接地板的介质基片上贴加导体薄片而形成的天线。它利用微带线或同轴线供电，在导体贴片与接地板之间激励起射频电磁场，并通过贴片四周与接地板间的缝隙向外辐射。

1. 微带环形天线的物理参数与等效电路

图 3.16 是矩形环形天线的几何示意图。

在天线电气参数计算中，矩形铜环可等效为与其面积相等的正方形铜环，微带铜线等效为一定半径的铜传输线。天线等效电路如图 3.17 所示，等效几何关系为

$$a' = \sqrt{a_1 a_2}\,,\ b' = 0.35b_1 + 0.24b_2 \tag{3.15}$$

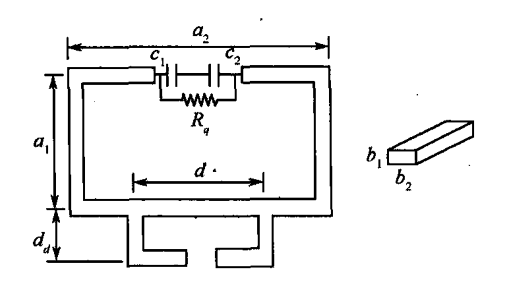


图3.16　矩形环天线的几何示意图

a_1—环形天线宽度；a_2—环形天线长度；

b_1—PCB覆铜厚度；b_2—PCB覆铜宽度。

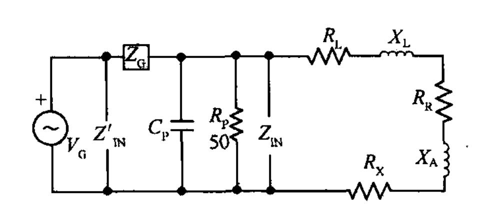


图3.17　等效电路

R_R—辐射电阻；R_L—损耗电阻；

R_X—附加损耗电阻；L_A—天线环路电感；

L_L—微带天线等效电感；Z_{IN}—输入阻抗；

Z'_{IN}—包含Cp在内的等效输入阻抗。

环形面积为

$$A' = a'^2$$

天线的输入阻抗为

$$Z_{IN} = (R_R + R_L + R_X) + j2\pi f_0(L_A + L_L) \tag{3.16}$$

$$R_R \approx 31171 \times \left(\frac{A'}{\lambda^2}\right)^2, \lambda = \frac{c}{f_0} \tag{3.17}$$

$$R_L = \frac{l_h}{P}R_S = \frac{a_1 + a_2}{b_1 + b_2}\sqrt{\frac{\pi f_0 \mu_0}{\sigma}} \tag{3.18}$$

$$R_X = \frac{2\pi f_0(L_A + L_L)}{Q} - R_R - R_L \tag{3.19}$$

式中：λ 为所选波长；f_0 为谐振频率；c 为光速；l_h 为微带铜环长度；P 为微带横截面的周长；R_S 为导体表面电阻；μ_0 为真空磁导率（大小为 $4\pi \times 10^{-7}$ H/m）；σ 为微带铜线的电导率，这里取电导率为 5.8×107S/m；Q 为品质因数。

电容 C_P 的寄生电阻是影响天线品质因数的主要因素，通过并联电阻 R_q 的方法调节天线的 Q 值，而且 R_q 还可以起到减小输入阻抗的作用，电容 C_P 与 Z_{IN} 并联可使天线发生谐振，则有

$$C_P = \frac{L_A + L_L}{(R_R + R_L + R_X)^2 + [2\pi f_0(L_A + L_L)]^2} \tag{3.20}$$

在谐振频率下，输入阻抗为

$$Z'_{IN} = R_R + R_L + R_X + \frac{[2\pi f_0(L_A + L_L)]^2}{R_R + R_L + R_X} \tag{3.21}$$

矩形铜环的环路电感可由正方形环近似求出，即

$$L_A = 2\mu_0 \frac{a'}{\pi}\left[\ln\left(\frac{a'}{b'}\right) - 0.774\right] \tag{3.22}$$

微带铜环的等效电感为

$$L_L = \mu_0 \frac{A'}{2a'} \tag{3.23}$$

天线的效率为

$$\psi = \frac{R_R}{R_R + R_L + R_X} \tag{3.24}$$

2. 天线通信距离计算

考虑信号反射、衍射、散射和偏极化等传播损失,实际通信距离为

$$R_d = \frac{\lambda}{4\pi\sqrt{\frac{T_L}{L_X\psi^2 P_{RF}}}}, P_{RF} = \frac{T_L}{L_X L_P \psi^2} \tag{3.25}$$

式中:R_d 为通信距离;L_X 为传播损失;T_L 为接收机灵敏度,发射天线与接收天线相同。

3.4 无线智能网络传感器研究中的若干问题

无线智能网络传感器研究中仍然存在以下主要问题:

(1)实时性问题。在工业测控系统中,网络的确定性是指通过网络传送的数据必须在确定的时间到达目的地,而以太网被认为是一种非确定性的网络系统,对于响应时间要求严格的控制过程会存在产生冲突的可能性,造成响应时间不确定,使信息不能够按要求正常传递。因此,实时性是必须考虑的问题。

(2)无线智能网络传感器节点时钟同步问题。监控系统多传感器信息融合时,上位机需要知道每个原始数据是何时采集的,采样的触发要求每一个节点有统一的时钟。

(3)通信策略问题。无线网络化智能传感器各节点之间的直接通信问题,主要涉及到各结点之间通信格式、通信机制以及通信速率等。

(4)底层网络接口(硬件接口)的实现问题——实现网络化。由于网络技术的迅猛发展,各类网络接口芯片为功能实现提供了大量的选择余地,但在选择和论证时要做到高可靠、低功耗、低成本和体积小等。

(5)高层网络接口(软件接口)的实现问题——实现内联网/因特网化。为保证智能传感器与网络上其他传感器或计算机之间实现可靠的数据通信,以及方便应用已有网络平台和相关成熟的网络技术,应选择成为事实标准的 TCP/IP 协议作为高层接口。用软件实现的 TCP/IP 标准接口使得网络化智能传感器具有高度的整体组态性(包括远程),把 TCP/IP 作为一种嵌入式应用,即把 TCP/IP 协议嵌入到智能传感器的 ROM 中,使得信号的收发都以 TCP/IP 方式进行。

(6)数据校正和智能标定算法问题。数据校正和智能标定是网络化智能传感器精确转换被测量为工程量的关键,只有选择了合适的校正模型和校正引擎,才有可能实现标准工程量的精确变送。校正引擎的设计不仅与具体变送器的特性有关,还与网络化智能传感器系统资源有关。设计校正引擎必须综合考虑各种因素,力求达到最佳效果。

(7)相关的工具需要进一步开发。为了方便用户配置传感器的功能,主要是对 TEDS

的读写,必须开发 TEDS 设计工具。

以上几个方面是无线智能网络传感器需要进一步研究的方向,相信随着这些问题的解决,无线智能网络传感器的功能会更加强大、性能会更好、应用会更广泛。

参 考 文 献

[1] Hill J L, Culler D E. Mica: A Wireless Platform for Deeply Embedded Networks[J]. IEEE Micro,2002,22(6):12 -24.

[2] Mica[OL]. http://www.xbow.com/products/wproductsoverview,aspx. 2006,7.

[3] http://www.wsn.net.cn. 2007,5.

[4] http://www.sia.ac.cn. 2006,11.

[5] 张劼,景博,张宗麟,等. 基于嵌入式 Web Server 的无线传感器网络系统设计[J]. 传感技术学报, 2006,19(2): 468 -472.

[6] Bo Jing,Jie Zhang ,Zheng Qin. Design of Micro Wireless Network Measurement and Control Server Based on ARM and μC/OS-Ⅱ[A]. The 6th World Congress on Intelligent Control Automation (WCICA06)[C]. IEEE Robotics and Automation Society, 2006,6:4453 -4458.

[7] Gerald F Ross et al. Batteryless sensor for intrusion detection and assessment of threats. Defense Nuclear Agency Technical Report DNA - TR - 95 - 21. Springfield, VA: National technical information service. 1, November, 1995.

第 2 篇

无线传感器网络体系结构与拓扑结构

第4章　无线传感器网络概述

1991年,Mark Weiser提出了普适计算(Pervasive Computing)的思想,基本思想是为用户提供服务的普适计算技术从用户意识中彻底消失,用户在潜意识上和周围环境进行交互,即把计算机嵌入到无数大大小小的信息设备当中,使人们注意中心回归到要完成的任务本身,并可以随时随地和透明地获得数字化的服务。实现普适计算要求从技术上有所突破,包括无线通信技术、移动通信技术、多种类异构网络互联技术、信息采集技术、微小型信息设备制造技术及其在这些设备上运行所需的软件技术,如嵌入式操作系统、轻量级网络互联协议和中间件等。

随着无线传感器网络(Wireless Sensor Networks,WSNs)的兴起与迅速发展,普适计算的技术理念在无线传感器网络平台上得到了很好的实践和延伸。作为实现普适计算的一个重要途径,无线传感器网络集信息采集、通信和计算能力于一身,能够很好地实现环境信息的感知,实现多通道交互方式。同时,通过现有的网络基础,如公共数据网、小型的局域网等传输媒介,实现服务数据的传输,最后终端用户通过普适设备来随时随地获取所需要的各种服务信息。

无线传感器网络是多学科高度交叉、新兴、前沿的一个重要研究领域,涉及传感器技术、网络通信技术、无线传输技术、嵌入式技术、分布式信息处理技术、微电子制造技术、软件编程技术等,它是继互联网之后,将对21世纪人类生活方式产生重大影响的IT技术之一。如果说互联网构成了逻辑上的信息世界改变了人与人之间的沟通方式,那么无线传感器网络就是将逻辑上的信息世界与真实的物理世界融合在一起,让人们可以自由地穿行于物理世界和信息空间。可以预见,在无线传感器网络这个充满着智能的普适计算环境中,未来客观世界的直接感知任务将由遍布四周的传感器网络来完成。那时,任意的时间,任意的地点,与外界信息的交流将变得更加方便,而且无线传感器网络利用天然的传输媒介,把普适计算的透明性显著表现出来,人类认识世界的能力将更加细致、深入。因此用无线传感器网络来实现普适计算是可行的,而且也是普适计算发展的趋势,这一切都将深刻地改变着人类与自然的交互方式。

4.1　无线传感器网络的概念、特点及应用

4.1.1　无线传感器网络的概念

近年来,关于具有群体能的无线传感器网络和基于无线传感器网络的自主智能系统的研究不断深入,但目前对它还没有一个公认的标准定义。有的认为它是一组通过无线网络连接起来的用于监测某种现象的传感器[2];有的认为它是具有计算、通信和协同能力的传感节点集合;有的将它定义成通过无线网络技术组织起来的一组传感节点,并能够

相互协同完成某一具体任务；有的认为是一组以 Ad hoc 方式组织起来的包括传感器的特殊无线网络；有的则从服务角度对它进行了讨论。这些观点或定义主要是从网络基础设施和传感器连接方式的角度对无线传感器网络的含义进行了阐述，但随着研究的不断深入和应用领域的拓展，仅从上述角度定义无线传感器网络是不够的。本文结合编者的理论研究与工程实践，理解无线传感器网络的概念如下。

【定义 4.1】无线传感器网络：由大量廉价的同构或异构，具有无线通信与计算能力的微型传感器节点，部署在无人值守的监控或测量区域，能够根据监测目标或对象自主完成给定任务，并将准确的信息传送到远程用户的智能监测网络系统。

该系统目的是协作地感知、采集和处理网络覆盖区域里被监测对象的信息，并发送给观察者，使人们在“任何时间、任何的点和任何环境条件”下都能够获取大量详实可靠的信息，并通过实时动态感知、认知而决策于物理世界。未来的传感器网络就是智能微粒群的集合，随机地散布在人类感兴趣的物理世界中，有的网络节点甚至可以像灰尘一样在空气中浮动，因此，人们又形象的比喻无线传感器网络为智能灰尘。随着无线传感器网络技术的不断发展，它最终成为一种无处不在的传感技术。

由定义 4.1 可以理解到，无线传感器网络的构成包括感知目标、网络节点、用户和其他网络等几部分。大量网络节点又可分为传感节点（Sensing Node）、簇头节点（Cluster-head Node）和 Sink 节点，亦称网关节点（Gateway Node），节点相互关系如图 4.1 所示。

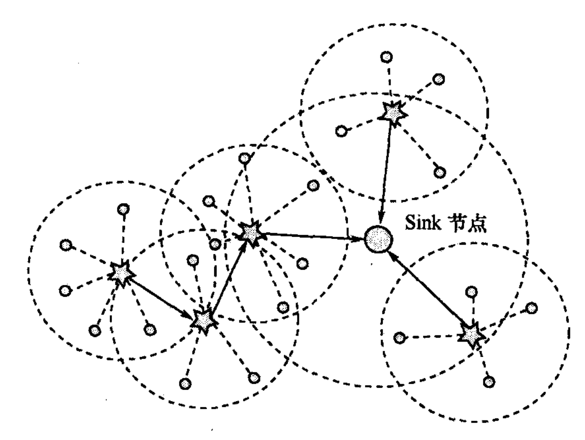


图 4.1　网络节点构成及相互关系

☆—簇头节点；○—传感节点。

图 4.1 中，各种实体的具体定义如下。

【定义 4.2】感知目标：面向应用的信号源，是无线传感器网络的感知对象，通过目标的热、红外、声纳、雷达或的震波等信号，能获取包括温度、湿度、噪声或运动方向和速度等目标属性。一个传感器网络节点可以感知网络分布区域内的多个对象，一个对象也可以被多个传感器节点网络所感知。

【定义 4.3】传感节点：在无线传感器网络中，每个传感节点既是传感器、又是路由器，具有原始数据采集、本地信息处理、无线通信和路由转发及与其他节点协同工作的能力，但其计算能力、存储能力、无线通信能力和电源供应是有限的。

【定义 4.4】簇头节点：簇头节点作为数据聚集和路由节点，将接收到的数据向 Sink 节点转发，簇头可预先指定，也可由节点使用分簇算法自动选举产生。

【定义 4.5】Sink 节点：亦称网关节点，是网络中的一类特殊节点。节点的数量通常很少，具有发布命令和收集数据的功能。在网内作为接收者和控制者，被授权监听和处理网络的事件消息和数据，可向网络发布查询请求或派发任务。面向网外，它可作为中继和网关，通过因特网或者卫星链路连接远端控制单元和用户。

【定义 4.6】观察者：观察者是传感器网络的用户，是感知信息的接收和应用者。一个无线传感器网络可以有多个观察者，一个观察者也可以是多个无线传感器网络的用户。观察者可以主动地查询或收集网络的感知信息，也可以被动的接收网络发布的信息。

无线传感器网络是一种全分布自治系统。通过随机抛撒的方式，大量传感器节点被密集部署于监控区域。这些传感器节点集成有传感器、数据处理和通信模块，它们通过无线信道连接，自组织地构成网络系统。传感器节点借助于其内置的数量不等的同构或异构传感器，探测环境中包括温度、湿度、压力、流量、转速、高度、速度、大小、方向、噪声、光强、频率、电磁频谱成分等众多人们感兴趣的物理现象。传感器节点间具有良好的协作能力，通过局部的数据交换来完成全局任务。通过网关节点，传感器网络还可以连接到现有的网络基础设施上，如因特网、以太网、移动通信网络等，有效拓展网络拓扑空间，使更大范围的授权近、远端用户实时共享采集到的信息。

由于无线传感器网络强调的是无线通信、分布式数据监测与处理和传感器网络，因此具有以下突出优势：

(1)由于集成了多种类型的传感器，增强了监测的性能。

(2)解决了布置在恶劣监测环境中的传感器的维护与更换问题。

(3)由于网络系统可以包括大量的传感节点，增强了系统的容错性，从而成倍地增加了对整个系统进行诊断的可靠性。

(4)通过大量无线传感器在监测区域附近的布置，通过分布监测来进行监测的效果要远优于仅使用单个传感器。

(5)通过分布式数据处理，即传感节点与簇头在局部进行协同计算，簇头将用户需求和部分处理过的数据通过数据聚集后进行传送，减少了数据传送量，尤其在距离较远时减少了无线电信号传送时消耗的能量。

(6)无线链路组建快速，无需架线挖沟，线路开通快。

(7)无线通信覆盖范围大，几乎不受地理环境限制，并可提供 64Kb/s ~ 11Mb/s 的通信速率，误码率低于 10 - 10E。

(8)可根据应用需求灵活制定网络规模与拓扑，并可随时增加链路，安装、扩容方便。

(9)无线链路安全性能高，可有效防止窃听。

(10)与有线网络相比，投资成本低、工程周期短、性价比高。

4.1.2　无线传感器网络的特点

无线传感器网络节点间具有很强的协同能力，从系统整体行为而言，网络系统是智能的，并且由于网络分布协作性和对等性测量的特点，其测量精度更高、范围更广、操作更为灵活，因此，无线传感器网络节点具有可测量、网络化、可嵌入三大特性，如图 4.2 所示。

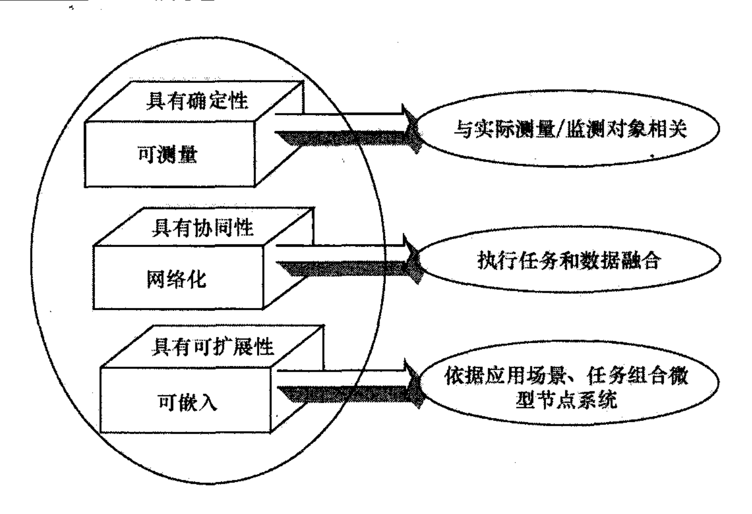


图4.2 网络节点的特性

在无线传感器网络的初期研究中,人们普遍认为,“成熟的因特网技术加上无线自组织网络的机制,对无线传感器网络的设计是足够充分的”。但随着研究的不断进展和深入,在技术需求和应用需求方面,无线传感器网络渐显出与无线自组织网络的明显不同:无线自组织网络致力于在不依赖于任何基础设施的前提下,为用户提供高质量的数据传输服务为目标,即以传输数据为目的;而无线传感器网络以监控物理世界为主要目标,将能源的高效使用作为首要设计出发点,专注于从外界获取有效信息,即以数据为中心。

可以说,无线自组织网络是一种数据网络,而无线传感器网络是一种测控网络。无线传感器网络具有以下区别于无线自组织网络的显著特征。

(1)面向应用。无线传感器网络是与应用领域密切相关的网络,它是针对某个或某些应用而专门设计的,不同应用关心不同的物理量,不同应用领域对数据采集、处理、传输的要求有很大差异,并且其硬件平台、软件系统和通信协议也必然会有很大差异。此外,应用领域的环境特点也对系统有很大影响。例如,地震预警系统和环境污染监测系统在网络拓扑结构、通信模型、数据传递模型等方面都有很大差别;另外,以可靠性和工作质量为主要指标的无线传感器网络,其网络节点数量级高,邻居节点的数据具有相似性,在数据传输路径需要进行数据融合,以减少冗余数据的发送,节省网络资源。因此,无线传感器网络不能像因特网那样有统一的通信协议平台,只有针对每一个具体的应用来开展设计工作,才能实现高效、可靠的系统目标,这也是无线传感器网络设计不同于传统网络的显著特征。

(2)网络规模大、节点密度高。为尽可能实时获取更精确、更完整、更有效的信息,网络节点通常密集部署于监测区域,其节点的数量和密度较无线自组织网络成“数量级”提高。无线传感器网络并非依靠单个节点能力的提升而是通过大量冗余节点的协同工作来提高网络系统的工作质量。

(3)节点能量、计算、存储及通信资源有限。能量受限是无线传感器网络的基本特征,网络节点只能携带有限的电池能量,且在应用过程中很难或不可能更换电池,尤其是在恶劣环境中运行,而数据采集、处理、传输及路由计算等都会消耗大量能源。传感器节点消耗能量的模块包括传感器模块、处理器模块和无线通信模块,其中绝大部分的能量消

耗在无线通信模块上，通常 1bit 信息传输 100m 距离所需的能量大约相当于执行 3000 条计算指令所消耗的能量[1]。能源的衰减会直接影响整个网络系统的寿命。由于廉价微型的传感器节点带来了处理器能力弱、存储器容量小的特点，在计算、存储能力等方面也是受限的，使得其不能进行复杂的计算，节点具有有限的硬件资源。另外，节点通信能力也是有限的，随着通信距离的增加，能耗会急剧增加[3]。基于节能需求，无线传感器网络应采用多跳路由的通信传输机制，尽量减少单跳通信的距离。由于无线信道自身的物理特性，通常使得它所能提供的网络带宽相对有线信道要小得多。此外，节点能量的变化、周围地势地貌以及自然环境的影响，使得网络的无线通信性能也会经常变化，甚至通信有可能时断时续。因此，如何设计可靠的通信机制以满足网络的通信需求是无线传感器网络所面临的一个重要挑战。

(4)以数据为中心。传感器网络关注的是具有某种特性的数据，它以数据本身作为查询或传输的线索，整个网络相当于分布式的网络数据库。传感器数量很多，种类、功能各不相同，采集到的数据数量巨大，要查询的数据分布在部分或所有节点中。在无线传感器网络中，人们通常只关心某个区域内某个观测指标的数值，而不会去具体关心单个节点的观测数据。例如，人们可能希望知道"监测区域某个方位或空间上的温度是多少"，而不会关心"具体某个节点所探测到的温度值是多少"。这就是无线传感器网络以数据为中心的特点，它不同于传统网络的寻址过程能够快速、有效地组织起各个节点的信息并融合提取出有用信息直接传送给用户。用户使用传感器网络查询事件时，直接将所关心的事件通告给网络，而不是通告给某个确定编号的节点。网络在获得指定事件的信息后汇报给用户，这种以数据本身作为查询或传输线索的思想更接近于自然语言交流的习惯。

(5)系统动态性强。无线传感器网络的动态性主要体现在系统本身、被监测对象和用户几方面。无线网络连接本身就有一定不稳定性，由于自然环境、能源等的影响，网络节点会因失效而离开网络，也会因某种需要而随时加入网络，从而引起网络拓扑结构的变化。此外，被监测对象本身会发生变化，用户位置也会发生移动。而无线传感器网络可实现自动组网，还具有网络自动配置和自动维护功能，因此可以有效保证网络的通信质量。

(6)多跳路由。网络中节点的能源非常有限，因此其通信覆盖范围一般只设定为几十米，若与通信覆盖范围外的节点通信，则需要通过中间节点进行多跳路由。

(7)快速部署。无线传感器网络具有可快速部署的特点，节点一旦被抛撒即以自组织方式构成网络，无需任何预设的网络设施。

(8)可靠性。传感器节点可以大规模部署于指定的恶劣环境或无人区域，由于传感器节点往往在无人值守的状态下工作，网络维护十分困难，甚至无法实现。因此，要求传感器节点非常坚固、不易损坏，在环境因素变化不可预知的情况下能够很好地适应各种极端的环境，如电磁干扰、电磁瘫痪等。

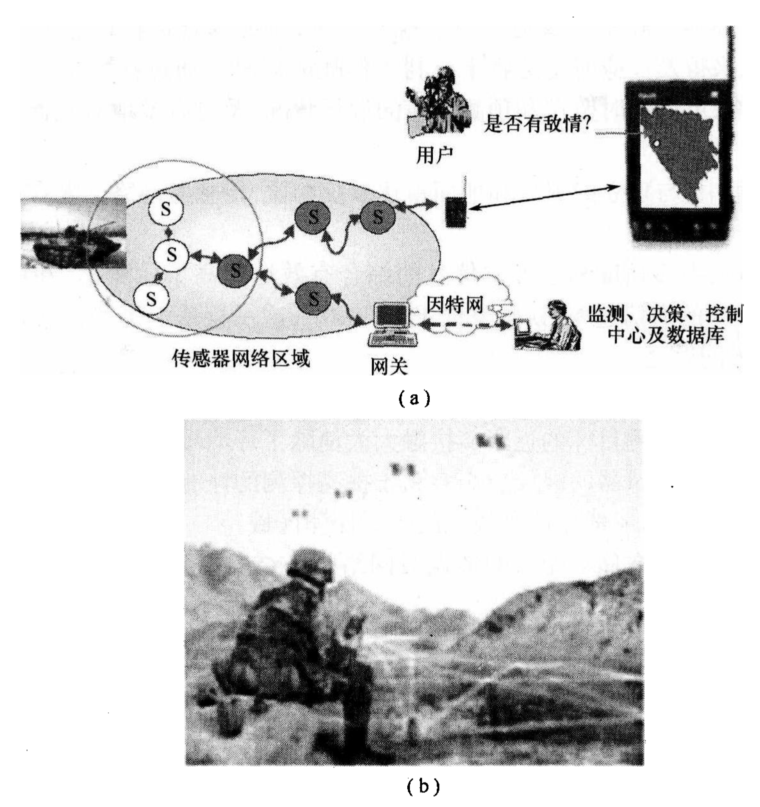
此外，为防止监测数据被盗取和获取伪造的监测信息，网络安全也十分重要，这要求无线传感器网络的设计必须具有很好的鲁棒性、容错性和可靠性。

4.1.3　无线传感器网络的应用

4.1.3.1　军事应用

无线传感器网络研究最早起源于军事领域，它利用低成本、低能耗、可计算的网络节

点收集、处理用户感兴趣的监测对象的数据，并在此基础上形成满足用户需求的高层应用。无线传感器网络具有部署快速、抗毁性强、隐蔽性强、覆盖区域大、监测精度高和容错性强等特点，因此，非常适合在军事上应用。无线传感器网络典型军事应用如图4.3所示。



(a)

(b)

图4.3 无线传感器网络典型军事应用

无线传感器网络是由密集型、低成本、随机分布的节点组成的，自组织性和容错能力使其不会因为某些节点在恶意攻击中的损坏而导致整个系统的崩溃，这一点是传统的传感器技术所无法比拟的，这使得传感器网络非常适合应用于恶劣的战场环境中，包括监控兵力和装备部署、战场的实时监视、侦察敌方地形和布防、战场评估。

无线传感器网络可通过飞行器撒播、人工埋设和火箭弹射等方式快速部署，节点的自组织能力和强大的容错能力将成为"网络中心战"不可或缺的组成部分，为组建传感器信息栅格、构建数据链和集命令、控制、通信、计算、智能、监视、侦察和定位于一体的 C^4ISRT (Command Control Communication computing Intel ligence Surveillance Reconnaissance and Targeting)战场指挥系统，实现战场无人值守、数字化边防等未来高技术信息国防与高技术信息战争提供有力的理论与技术支持。

传感器网络可以通过分析采集到的数据，得到十分准确的目标定位与目标识别，为火控和制导系统提供精确的制导。在生物和化学战中，利用生物和化学传感器，传感器网络可以实施核、生物和化学攻击的侦察和搜索，及时、准确探测到生化武器的成分并提供情报信息，为我军提供宝贵的反应时间，从而最大可能的减小伤亡，传感器网络也可避免核

反应部队直接暴露在核辐射的环境中。

战场上的指挥员往往需要及时准确的了解部队、武器装备和军用物资供给的情况，铺设的传感器将采集相应的信息，并通过 Sink 节点将数据送至指挥部门，通过融合来自各战场的数据形成完备的战区态势图。通过铺设传感器网络，还可以更隐蔽、近距离地观察敌方的布防，对冲突区和军事要地进行监视。当然，也可以直接将传感节点撒向敌方阵地，在敌方还未来得及反应时迅速收集有利于作战的信息。通过在大型复杂武器装备上铺设传感器网络，可以实时监控和预测装备的运行状况，及时有效地对武器装备进行故障诊断与预警。

在军事应用中，与独立的卫星和地面雷达系统相比，传感器网络的潜在优势表现在以下几个方面：

(1)分布节点中多角度和多方位信息的综合有效地提高了信噪比，并可提供从十几 Kb/s ~ 几十 Mb/s 的通信速率，误码率低于 10 - 10E，这一直是卫星和雷达这类独立系统难以克服的技术问题之一。

(2)传感器网络低成本、高冗余的设计原则为整个系统提供了较强的容错能力。

(3)传感节点与探测目标的近距离接触大大消除了环境噪声对系统性能的影响。

(4)节点中多种传感器的混合应用有利于提高探测的性能指标。

(5)多节点联合，形成覆盖面积较大的实时探测区域。

(6)借助于个别具有移动能力的节点对网络拓扑结构的调整能力，可以有效地消除探测区域内的阴影和盲点。

4.1.3.2　非军事应用

无线传感器网络的应用已由军事领域扩展到其他许多领域，能够完成诸如环境监测、灾难预警与救助、家庭健康监测、智能家居、商务应用、建筑物状态监控、空间探索等传统系统无法完成的任务。

1. 环境科学

随着人们对环境的日益关注，环境科学所涉及的范围越来越广泛。传感器网络在大型生态多样性研究方面，为野外随机性的研究数据获取提供了极大的方便。它可用来研究环境变化对气候、农作物、动物的影响，监测大气、海洋和跟踪候鸟和昆虫的迁移等。同样，传感器网络对森林火灾准确、及时预报也是及其有效的。目前，传感器网络在精细农业中的应用越来越多地受到重视，美国、日本、中国等国家都在积极开展以监测农作物中的害虫、土壤的酸碱度、灌溉和施肥状况等精细农业的研究与应用。典型应用如图 4.4 所示。

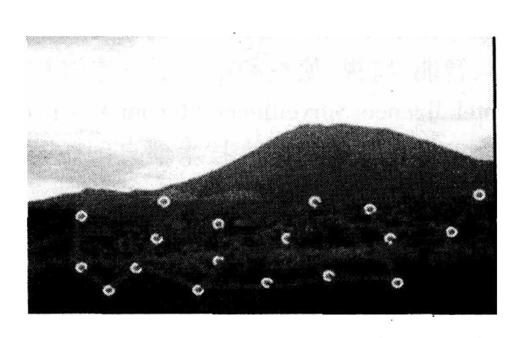
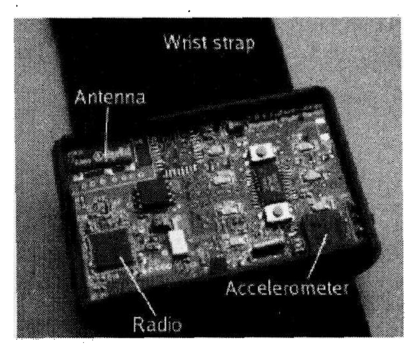


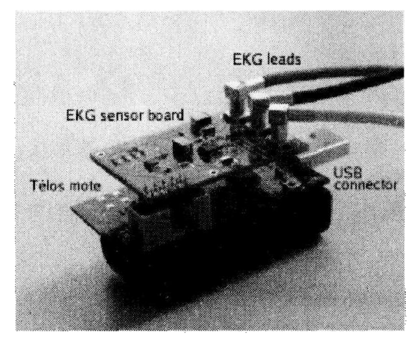


图 4.4　无线传感器网络在环境监测和精细农业中的应用

2. 医疗卫生

如果在住院病人身上安装特殊用途的传感节点，如心率和血压监测设备，利用传感器网络，医生就可以随时了解被监护病人的病情，使医生尽早的发现病症，进行及时处理。医生利用分散的传感节点来监测病人，为未来大规模远程医疗提供技术实现手段。图 4.5 为用于医疗的无线传感节点。





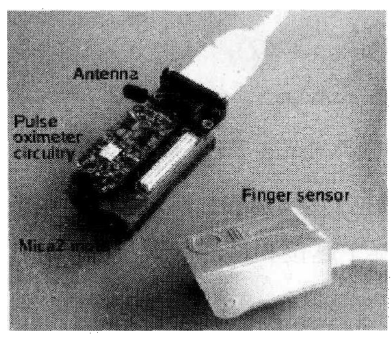


图 4.5　用于医疗的无线传感节点

还可以利用传感器网络长时间的收集人的生理数据，这些数据在研制新药品的过程中是非常有用的。与医疗处置中心相比，无线传感器网络推动了智能健康家庭的建设，提高了人们的生活质量。

3. 商务应用

自组织、微型化和对外部世界的感知能力是传感器网络的 3 大特点，这些特点决定了传感器网络在商业领域应该也会有不少的机会。例如，在灾难拯救、仓库管理、交互式对象、工厂过程控制与自动化、产品质量监测、构建智能办公环境、智能楼宇、设备诊断、防盗系统、车辆追踪与监控、材料疲劳监测、机械的故障诊断、制造业中对机器人的控制和引导等众多领域，无线传感器网络都将会孕育出全新的设计和应用模式。

(1)办公室环境控制。大部分办公室内的空调都是中心控制的。由于单控制器的中心系统产生的气流分布不均匀，会造成房间内某区域的温度比其他区域的温度高。可以在房间内安装无线传感器网络来控制不同区域的温度。

(2)互动博物馆。将来，孩子们可以通过与博物馆中的展品互动来学习更多的知识。这些展品可以对孩子们的触摸和声音做出响应。孩子们也可以参与一些互动式的科学实验。另外，无线传感器网络还可以在博物馆中提供无线寻呼和定位，便于对参观者进行管理和监控。

(3)车辆防盗系统。传感器节点可以监测车辆周围一定范围内的安全威胁,并通过因特网向远程的车主报告。

(4)存货管理。在仓库的每项存货中安置传感器节点。管理员可以方便地查询存货的位置和数量。在增加存货时,管理员只需在存货中安置相应的传感器节点。在日常管理中,管理员可以在控制室实时监测每项存货的状态,如图 4.6 所示。

(5)车辆追踪与监控。目前有两种应用无线传感器网络进行车辆追踪与监控的方法。一是在传感器网络内部,对数据进行本地分析,然后将计算出的车辆位置传给监测点;二是各传感器节点将原始数据直接传给监测点,由监测点计算车辆的位置,如图 4.7 所示。



图 4.6　无线传感器网络用于存货管理

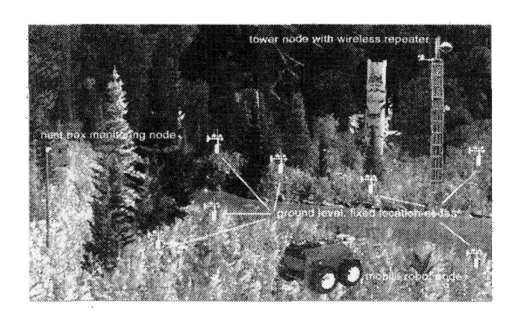


图 4.7　无线传感器网络用于车辆追踪

(6)德国某研究机构正在利用传感器网络技术为足球裁判研制一套辅助系统,以减小足球比赛中越位和进球的误判率。

4. 家庭应用

嵌入家具和家电中的传感器与执行机构组成无线网络,网络节点可以彼此交互,或与因特网连接在一起与外部网络交互,使用户可以方便的对家电进行远程监控。从而为我们提供更加舒适、方便和具有人性化的智能家居环境。

5. 空间探索

可用飞行器将网络节点散布在太空中,对空间碎片和太空环境实时监测。探索外部星球一直是人类梦寐以求的理想,借助于航天器布撒的传感器网络节点实现对星球表面长时间的监测,是一种经济可行的方案。

4.2　无线传感器网络与现有网络比较

由于无线传感器网络是一种测控网络,以监测物理世界为主要目标,其具有与传统有线和无线网络,如现场总线、因特网、移动通信网、Ad hoc 等网络有较大的不同,有别于其他网络的主要特征包括以下几个方面:

(1)传统网络设计遵循端到端的边缘论思想,强调将一切与功能相关的处理都放在网络的端系统上,中间节点仅负责数据分组的转发,而无线传感器网络的节点具有数据处理与计算功能。

(2)传统网络以传输数据为目的,无线传感器网络以数据为中心。

(3)与传统的 Ad hoc 网络相比,无线传感器网络具有与感知目标紧密耦合、传感节点

分布式自主管理等明显特征。

(4)传统网络的发展趋势是电信网、计算机网及电视网的逐步融合,而无线传感器网络是与应用领域密切相关的网络,它是针对某个或某些应用而设计的。

(5)与传统无线网络相比,无线传感器网络以静态网络为主,节点一般不进行快速移动,但节点可能会随时加入或离开,因而网络的拓扑变化很快。

(6)无线传感器网络中节点资源有限,其能源供给、计算和存储能力与传统网络明显不同。

(7)与有线网络相比,投资成本低、工程周期短、性价比高。

本节重点比较无线传感器网络与现场总线和 Ad hoc 的区别。

4.2.1 无线传感器网络与现场总线的区别

现场总线是一种典型的测控网络,是为实现在严格的实时约束下工作而特别设计的,作为控制环路的一部分,容错性是其优越性的体现。典型总线有自动化控制领域的 Profibus 现场总线和 IEEE802.4 令牌环总线网络、机载或车载的 CAN 总线网络,但由于严格的实时性需求,这些网络的构建以有线方式为主。对应 OSI 参考模型,现场总线只利用了物理层,数据链路层和应用层,避免了数据多跳通信延迟和节点关联队列延迟。尽管固有有限差错率不利于实时性,但目前人们仍然致力于在无线通信上实现现场总线的构想。

首先,由于现场总线通过采集、传输和报告传感数据来控制物理对象或环境,因此,从相似性角度而言,两个研究领域之间的界限比较模糊,无线传感器网络可以被认为是无线现场总线的实例。但由于无线传感器网络是应用型网络,关注的焦点不是数十毫秒范围内的实时性,网络应用能够容许一定时间甚至是较长时间的延迟和延迟波动。其次,无线传感器网络的"自适应协议",如精度—能量效率比等在现场总线中是一个生僻的概念。最后,也是最重要的一点,现场总线及其相关协议没有考虑网络系统能源的节约性,在降低能耗方面作为很少,而无线传感器网络的能耗指标却是其重要的指标之一。

4.2.2 无线传感器网络与无线自组织网络的区别

无线自组织网络是为了满足日益增加的通信需要而提出的,而无线自组织网络的概念与无线多跳通信直接相关,作为一个典型要素,无线自组织网络指出了网络参与节点的移动性。这种网络可应用在抢险救灾现场、股市交易所、不适宜铺设通信电缆的地点等,与直接的信源到信宿的通信相比,这种网络能够覆盖更大的区域。无线自组织网络和无线传感器网络比较,在概念和功能上存在本质上的差异。

(1)应用特征。无线自组织网络与不同的应用及用户设备相关,以数据为应用特征,在典型无线自组织网络应用中,无线自组织网络用于两个远端对等实体间的语音通信,或者访问远程内部结构(如一个网络服务器),接入节点数量动态变化大(进入网络、退出网络、快速移动、静止等)。由于采用了高能电池,无线自组织网络终端可以采用笔记本电脑或 PDA(手持设备),所以,为了支持这些应用,设备必须足够强大。而无线传感器网络针对提供服务的特殊应用特征,融合了大量的传感、计算和通信技术,其前端均采用小型化,甚至是微型化、微粒化设备,自适应的协议也必须适合不同的网络密度(稀疏的或密集的),而在无线自组织网络中自适应协议的要求并不显著。

(2)环境交互性。无线传感器网络必须与环境进行交互,其通信需求与人时刻参与的测控形式网络有很大不同。在无线传感器网络中,可能在很长一段时间内数据产生率或数据传输率都非常低,而某个事件突发所带来的网络通信量激增,将会导致网络数据拥塞。此外,无线传感器网络中,长期(数月)的休眠与短期(数秒或数分钟)的高度活跃交替,将容量逼近极限值,而无线自组织网络利用已知的通信特性,可用于支持比较常规的应用(如网络、语音等)[4]。

(3)测量。无线传感器网络拥有成千上万的测量实体,要求测量方案简洁、有效,冗时性和实时性可自由设置,而且不必为每个传感器节点配置唯一的 ID(IDentifier)标识,相对测量成本降低;而 ID 识别器在 Ad hoc 网络中是一种合理的设置,且是有必要的[5]。

(4)能源。无线传感器网络对网络的工作寿命有更苛刻的要求,而且与无线自组织网络相比,充电或更换网络节点电池有可能是非常困难,甚至是无法实现的。尽管无线传感器网络和无线自组织网络中,均存在电源供应不足的问题,但与无线自组织网络比较,电源对无线传感器网络整个系统结构的影响更加深远。

(5)可靠性和服务质量。无线自组织网络与无线传感器网络在可靠性和服务质量方面的要求有明显的不同,无线自组织网络中每个节点应该是非常可靠的;无线传感器网络中单个节点之间几乎不相关。无线自组织网络的服务质量是由传统应用规定(如语音应用中的低抖动)[6],而无线传感器网络需要在考虑电源的基础上,建立全新的服务质量概念。

(6)以数据为中心。在无线传感器网络中,冗余部署使得以数据为中心具有吸引力。该概念与无线自组织网络是不同的。除非无线自组织网络中采用如文件共享之类的应用,这种应用与以数据为中心的方法具有类似之处,否则以数据为中心的协议与无线自组织网络是不相关的[7]。

(7)系统简化。由于传感器网络节点配置简单,而且能源供应有限,与 PC、工控机等相比,必须大大简化系统硬件、嵌入式软件和组网协议与算法命令,并打破传统的分层原则思想,以跨层设计为主要简化设计思想。对于无线自组织网络,系统资源(如内存、电源)与使用的重加权路由协议相关。而且加权路由协议的相关资源(如内存、电源)在随机量中是不可使用的,因此需要可观测的、能够有效利用资源的解决方案。

(8)移动性。无线自组织网络中的移动性是指网络节点的移动和多跳路径改变;而在指定的无线传感器网络应用中,某些传感器节点是可移动的,才存在多跳路径改变等问题。此外,无线自组织网络和无线传感器网络中的移动性是相互关联的,一组节点按照某种相关的类似形式移动。这种相关性可在无线自组织网络中发生,正如一群人一起去旅游;可在无线传感器网络中发生,节点的移动是相互关联的,节点会随着暴风、河流等载体一起移动。

总之,无线传感器网络作为一个与无线自组织网络相异的系统概念,其应用必须与物理环境发生相互作用,而且必须仔细确定将各种因素折中考虑的合理性。

4.2.3　无线传感器网络与无线自组织网络的共性

从无线通信网络技术诞生到现在,尤其是在过去的 80 年间取得了突飞猛进的发展。主流的无线数据网络技术,如 IEEE802.11、Bluetooth、RF 都是为了数据传输而设计的,而

目前无线数据网研究的热点是无线自组织网络，作为因特网在无线和移动范畴的扩展和延伸，无线自组织网络可以实现不依赖任何基础设施的移动网络节点短时间地互联。

无线传感器网络与无线自组织网络有很多相似的特点：

(1)无中心、分布式。无线自组织网络中没有绝对的控制中心，所有节点地位平等，节点之间通过分布式的算法来协调彼此的行为，无需人工干预和任何其他预制的网络设施，是一个对等式网络。节点可以随时加入或离开网络，且任何节点的故障不会影响整个网络的运行，具有很强的可靠性和抗毁性。

(2)自组织性。通常网络所处物理环境及网络自身有很多不可预测因素。如节点的位置不能预先精确设定；节点之间的相邻关系预先也不知道；部分节点由于能量耗尽或其他原因而死亡，新的节点加入到网络中；无线通信质量受环境影响不可预测；网络环境中的突发事件不可控。因此，要求节点具有自组织的能力，可以在任何时刻、任何地方快速展开并自动组网，自动进行配置和管理，通过适当的网络协议和算法自动转发监测数据。

(3)拓扑动态变化。网络拓扑结构是指从网络层角度看物理网络的逻辑视图。网络中节点具有移动能力；节点在工作和睡眠状态之间切换以及传感器节点随时可能由于各种原因发生故障而失效，或者有新的传感器节点补充进来以提高网络的质量；无线收发装置的天线类型多种多样、发送功率随携带能量的变化而变化；加之无线信道间的互相干扰、地形和天气等综合因素的影响，移动终端之间通过无线信道形成的网络拓扑结构随时可能发生变化，而且变化的方式与速率难以预测。这就要求网络系统能够适应拓扑变化，具有动态可重构的性能。

(4)多跳路由。由于节点发射功率的限制，节点的覆盖范围有限，通常只能与其邻居节点通信，如果当要与其覆盖范围以外的节点通信时，需要通过中间节点的转发。此外，多跳路由是由普通网络节点协作完成的，没有专门的路由设备来完成。这样每个节点既可发起信息，也可转发信息。

(5)安全性较差。无线自组织网络是一种特殊的无线移动网络，由于采用了无线信道、自带电源、分布式控制等技术，网络更容易受到被动窃听、主动入侵、拒绝服务、剥夺“睡眠”等网络攻击。因此，网络通信保密性和安全性十分重要，信道加密、抗干扰、电磁兼容、屏蔽、用户认证和其他安全措施都需要特别考虑，以防止监测数据被盗取和伪造监测信息入侵等。

(6)传输带宽受限。由于无线信道本身的物理特性，采用无线传输技术作为底层通信手段所能提供的网络带宽相对有线信道要低很多。此外，由于竞争共享无线信道产生的冲突、信号衰减、噪声和信道间干扰等多种因素，实际带宽远远小于理论上的最大带宽。

(7)扩展性较差。拓扑结构的动态变化使得不同子网的移动终端可能同时处于一个无线自组织网络中，因而子网技术所带来的可扩展性无法应用到自组织网络中。

4.3　无线传感器网络关键技术及研究进展

4.3.1　无线传感器网络关键技术

无线传感器网络具有多学科交叉性，所需要研究的内容主要分为 4 个部分，包括网络

通信协议、核心支撑技术、自组织管理、开发与应用，每个部分都有许多关键技术需要研究与解决。

1. 网络通信协议

基于传感器节点能源、计算、存储和通信能力均十分有限的限制，每个节点只能获取到局部网络的信息，因而在实现完成任务功能的前提下，节点上所运行的通信协议应尽可能简单；同时，网络拓扑结构和外界环境的不断变化，也对网络通信协议的设计提出了更高的要求。无线传感器网络的通信协议包括物理层、数据链路层、网络层和数据融合层，各层相互配合运行，使得若干个独立的传感器节点能够形成一个多跳、动态的数据聚集网络。本书第7章~第9章对无线传感器网络各个层次的通信协议进行了全面、详尽的叙述。

2. 核心支撑技术

无线传感器网络核心支撑技术使用网络通信协议提供的服务，并通过应用服务接口来屏蔽底层网络细节，使网络授权用户可以方便的对无线传感器网络进行操作。无线传感器网络依靠这些丰富的核心支撑技术构成了一个具体的面向特定应用的网络系统。

无线传感器网络的核心支撑技术包括体系结构、拓扑控制、节点定位、时间同步、网内信息处理、连通与覆盖、网络可靠性、网络安全、服务质量、系统软件、应用软件等主要内容。本书分别对这些核心支撑技术进行了全面、详尽的阐述和论证。

3. 自组织管理

网络拓扑的多变性和网络环境状况及外在环境要求无线传感器网络具有自组织的能力，能够自动组网运行、自行配置维护、适时转发监测数据。自组织管理技术使用网络通信协议提供的服务，通过网络管理接口来屏蔽底层网络的细节，使终端用户可以方便地管理配置无线传感器网络。

无线传感器网络的自组织管理技术包括节点管理、资源与任务管理、数据管理、初始化与系统维护管理等。

4. 开发与应用

作为一种源于应用而又服务于应用的现实可行的无线网络技术，无线传感器网络需要有一套完整的软硬件设计原则、有效的开发平台以及仿真平台、一系列别具特色的应用指导实例。本书的第4篇系统地描述了无线传感器网络的开发与应用环节所涉及的内容，包括仿真平台、硬件系统开发、操作系统、软件开发、环境监测应用及目标追踪应用等。

无线传感器网络的理论框架结构如图4.8所示，无线传感器网络的深入研究包括能量供给、数据存储、数据处理、数据传输、同步率、系统可靠性等诸多内容。为进一步提高无线传感器网络性能，需要对无线传感器网络的资源管理、信息融合、信息传输3个部分进行研究和优化。

资源管理主要包含传感器管理、过程管理、网络规划、网络和拓扑控制等，主要用于优化网络性能、减少网络能耗、提高网络稳定性等。

信息融合主要包含传感器融合、数据融合、数据挖掘、相关性、估计和滤波跟踪等，用于提高网络的信息有效性和网络的协作信息处理能力。

信息传输主要包含物理编码、信道接入、数据路由、互联网接入、网络协议等，用于提

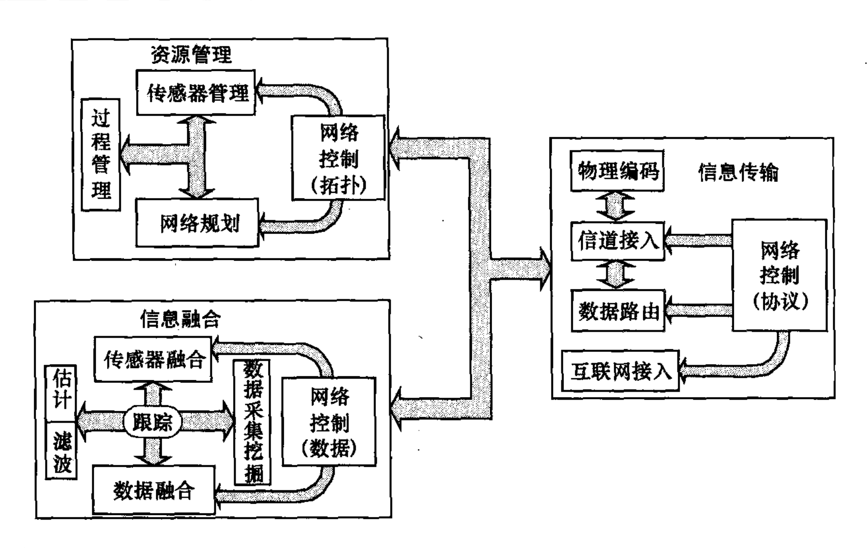


图 4.8　无线传感网络理论框架

高网络能量有效性,数据传输实时性和空间拓展。

目前,无线传感器网络技术还处在关键技术的试验验证阶段,相关应用的试验性相对突出,与在诸多领域大规模的实际应用还有相当的距离。

4.3.2　无线传感器网络国外研究进展

无线传感器网络的基本思想起源于 20 世纪 70 年代美国军方的作战需求。1978 年,DARPA(Department of Advanced Research Project Agency)在卡耐基—梅隆大学成立了分布式传感器网络工作组,工作组根据军方对侦查系统的需求,研究传感器网络中的通信、计算问题。此后,DARPA 又联合美国国家自然科学基金设立了多项有关无线传感器网络的研究项目。这些研究推动了以网络技术为核心的新军事革命,建立了网络中心战的思想体系,并由此拉开了无线传感器网络研究的序幕。

20 世纪 90 年代中期以后,无线传感器网络引起了学术界、军事界和工业界的极大关注,美国通过国防部和国家自然基金委员会等多种渠道投入巨资支持无线传感器网络技术的研究,其他发达国家也相继启动了许多关于无线传感器网络的研究计划,代表性的研究计划包括以下几种:

(1)SensorIT 计划。DARPA 在 1998 年开展了名为 SensorIT(Sensor Information Technology)的研究计划,这个计划共有 29 个研究项目,分别在 25 个研究机构完成。SensorIT 的研究主要集中在两个方向,一是适应战场高度动态环境、建立快速进行任务分配和查询的反应式网络系统;二是发挥网络化观测优势的无线传感器网络协作信息处理技术。

(2)WINS 计划。1996 年由 DARPA 资助,加州大学洛杉矶分校与罗克韦尔研究中心合作开展 WINS (Wireless Integrated Network Sensors)研究。该研究计划的目标是结合 MEMS 技术、信号处理技术、嵌入式计算和无线通信技术,构造大规模、复杂的集成传感系统,实现物理世界与网络世界的连接。

(3)Smart Dust 计划。1998 年,在 DARPA/MTO MEMS 的资助下,加州大学伯克利分校 UCB 开始了名为 Smart Dust 的研究计划,其目标是结合 MEMS 技术和集成电路技术,

研制体积不超过 $1mm^3$，使用太阳能电池，具有光通信能力的自治传感器节点。由于体积小、重量轻，该节点可以附着在其他物体上，甚至可以在空气中浮动。

(4)SeaWeb 计划。SeaWeb 项目是由美国海军研究办公室(Office of Naval Research，ONR)支持，目标是研究基于水声通信的无线传感器网络的组网技术。该项目针对水声通信带宽窄、速率低、时延抖动大等特点给通信协议的设计带来了很大的困难，利用无线传感器网络获取的信息对水声信道时变、空变的特点进行建模。因此，该项目在1999年—2004年间进行了多次实验，取得了大量的现场数据，验证了水声传感器网络系统的可行性。

(5)Hourglass 计划。哈佛大学于2004年开展了名为 Hourglass 的研究项目，旨在构建一个健壮、可扩展的数据采集网络，即把不同的传感器网络连接起来，提供一个对广泛分布的传感数据进行采集、过滤、聚集和存储的框架，并致力于将这个框架推进成为一个可以部署多传感器网络应用的平台。其关键在于为异构的无线传感器网络提供"网格API"，通过网格计算以统一地存取传感数据。

(6)SensorWebs 计划。2001年以来，美国国家航空与航天局(National Aeronautics and Space Administration，NASA)的 JPL(Jet Propulsion Laboratory)实验室所开展的 SensorWebs 计划，致力于通过近地低空轨道飞行的星载传感器提供全天候、同步、连续的全球影像实现对地球突发事件的快速反应，并准备用在将来的火星探测项目上。目前，已经在佛罗里达宇航中心周围的环境监测项目中进行测试和进一步完善。

(7)IrisNet 计划。IrisNet 是 Intel 公司与美国卡耐基梅隆大学正在合作开发的技术，其主要设想是利用 XML 语言将分散于全球的传感器网络上的数据集中起来并加以灵活利用，使其成为传感信息世界中的 Google。在"搜索空停车场"的实例中，它在多个停车场里设置摄像头，并组成网络，根据所拍摄的录像建立停车空位信息数据库，为用户提供查询空车位的服务。

(8)NEST 计划。网络嵌入式系统技术(Network Embedded System technology，NEST)战场应用试验作为 DARPA 主导的一个重要项目，致力于为火控和制导系统提供准确的目标定位信息。该项目成功的验证了能够准确定位敌方狙击手的无线传感器网络技术。这些传感器节点能够跟踪子弹产生的冲击波，在节点范围内测定子弹发射时产生声振和枪振的时间，以判定子弹的发射源。三维空间的定位精度可达1.5m，定位延迟达2s，甚至能显示出敌方射手采用跪姿和站姿射击的差异。

(9)μAMPS 计划。μAMPS(micro-Adaptive Multi-domain Power-Aware Sensors)项目是由 MIT 承担，目标是设计节能、自组织、可重构的无线传感器网络。研究人员设计了低功耗的 μAMPS－Ⅰ、μAMPS－Ⅱ传感器节点和以节能、可重构为主要目标的系统体系结构。

除了标志性的研究计划及成果外，国外关于无线传感器网络的研究还取得了以下研究进展。

4.3.2.1　军事方面研究进展

1. 陆军方面

2001年，美陆军提出"灵巧传感器网络通信(Smart Sensor Network Communication，SSNC)"计划，被批准在2001—2005财政年度期间实施。2004年，美陆军又提出了"无人职守地面传感器群"和"战场环境监视系统"。2005年5月，美国防部推出《信息安全：增

强传感器网络的控制》报告，具有指导意义地阐述了美国未来发展计划。中情局的风险投资公司 InQ - Tel 已购买了微尘网络公司的股份，美国国土安全部研究人员也已将微型传感器的研发列为最优先课题。

2. 空军方面

2002 年，美空军开始发展 MC2A 多传感器的指挥和控制飞机技术，希望将 E - 2C 机载预警与控制系统（AWACS）和 E - 8C 联合监视目标攻击雷达系统（J - STARS）的空中和地面监视、战场管理、指挥与控制、目标瞄准能力综合到同一架或几架波音 767MC2A 飞机上，该项目预计 2007 年完成。

3. 海军方面

美国海军最近开展的网状传感器系统 CEC（Cooperative Engagement Capability）是一项革命性的技术，海军为此投资近 20 亿美元，并已将部分成果用于新型攻击型潜艇 NSSN 中。CEC 是一个无线网络，其感知数据是原始的雷达数据，该系统适用于舰船或飞机战斗群携带的电脑进行感知数据处理。每艘战船不但依赖于自己的雷达，还依靠其他战船或者装载 CEC 的战机来获取感知数据。例如，一艘战船除了从自己的雷达获取数据以外，还从舰船战斗群的 20 个以上的雷达中获取数据，也可从鸟瞰战场的战机上获取数据。空中的传感器负责侦察更大范围的低空目标，这些传感器也是网络中重要的一部分。利用这些数据合成图片具有很高的精度。由于 CEC 可以从多方面探测目标，极大的提高了测量精度，利用 CEC 数据可以准确地击中目标。CEC 还可以快速而准确地跟踪混乱战争环境中的敌机和导弹，使战船可以击中多个地平线或地平线以上近海面飞行的超声波目标。因此，即使是今天最先进的反舰巡航导弹也会被实时地监测到并被击中。

另外，美国海军的海网 SeaWeb 水下声学网络是目前美国比较成功的水下传感器网络范例，2004 年—2006 年间已进行了第二阶段地多次改进试验。

4.3.2.2　非军事方面研究进展

2002 年 10 月，美国英特尔公司发布了用于环境、医疗、行星探测的基于微型传感器网络的新型计算发展规划。该计划包括物理阶段、实现阶段和应用阶段，物理阶段主要开发集成感知、计算和通信功能的超微型传感器，即 mote，计划 6 年完成。

美国工业无线共同体于 2002 年举办了“21 世纪的工业无线技术”研讨会，会上披露美国总统的科学技术咨询顾问早在 1997 年就断言，“无线传感器及网络的发展会提高 10% 的生产效率和减少 25% 的排放或泄漏”。

2003 年，英特尔公司伯克利研究实验室和加州大学伯克利分校合作，将安有 D 型微型电池的第二代传感器网络，布设于缅因州大鸭岛上，实现对敏感野生动物及其栖居地无入侵式及无破坏式的环境监测。

2004 年 8 月，微尘网络公司制造的 22 个传感器被安装在连锁零售店内，以监测店内温度和能源的利用情况。NASA 的 JPL 实验室研制的 SensorWebs 为将来火星探测进行技术准备。目前，该系统正在佛罗里达宇航中心进行测试和完善。

2003 年，美国能源部与许多大学和研究中心合作，资助 520 万美元研究利用无线和感知方法提高工作部门效率；资助 300 万美元研究分布式无线多传感器技术；与 Eaton 公司等合作，资助 300 万美元研究了 Eaon 无线传感网络的能量管理解决技术；资助 290 万美元研究如何利用低成本的一氧化碳传感器和火炉控制系统提高锅炉效率等；最近与美

国 Sandia 国家实验室合作，共同研究能够尽早发现以地铁、车站等场所为目标的生化武器袭击，并及时采取防范对策的系统。

从 2003 年开始，美国科学基金委员会就开始资助传感器和无线传感网络项目，涉及能感知有毒化学物品、爆炸物和生物攻击的传感器，在分布环境下的传感网络系统，传感器和工业系统的集成，以及在决策过程中如何有效利用感知数据的问题。这些研究和应用紧密联系，政府每年拨款 3400 万美元支持大小不同的研究项目。在 2005 年对网络技术和系统的研究计划中，主要研究下一代高可靠的、安全的可扩展的网络，可编程的网络及传感器系统的网络特性，包括研究体系结构、工具、算法以及应用系统，该项资金达到 4000 万美元。

2003 年 7 月，松下电器、NEC 及日立等 8 家企业宣布成立“IPv6 传感器网络联盟”，其宗旨是创建利用 IPv6 的新兴产业。2004 年 3 月，日本总务省宣布成立“泛在传感器网络”调查研究会。在欧洲第一届“无线传感器网络论坛”上，德国提出了一种只有豌豆大小的新型无线传感器网络系统，用于操纵机器人、监护病人及寻找事故中的死伤者，该系统是欧盟近年来的一项重要科研项目，由柏林工业大学、弗朗霍夫研究所及费迪南一布劳恩研究所共同研制。

欧盟的 EYES（自组织和协作有效能量的传感网络）是为期 3 年的一项计划，从 2002 年开始实施。研究的范围包括分布式信息处理、无线通信和移动计算。该项目集中研究体系结构、协议和软件，使节点“聪明”，自组织及相互协作。他们提出应具备的两层结构：低层处理传感器和传感网络。传感网络根据低层提供的信息，为应用提供服务。在通信网络方面，开发的新技术包括内部传感器结构、分布无线接入、路由协议、可靠的端到端传输、节点时间同步和定位；在服务层上，支持移动传感器应用，包括信息收集、查找、发现和安全等。2004 年 3 月，日本总务省成立泛在传感网络（Ubiquitous Sensor Network，USN）调查研究会，研究会成员除家电厂商、通信运营商和大学之外，还包括 SKYLEYNETWORKS、世康、欧姆龙等大型公司。

美国 Crossbow 科技公司推出了新一代无线传感器网络研发的硬件平台——Crossbow Imote2。Imote2 是由 Intel 公司与 Crossbow 公司联合开发，并由 Crossbow 发布。Imote2 的诞生使无线传感器网络节点的处理性能达到了一个新的高度。Imote2 集成了高性能、低功耗的 PXA271 Intel XScale 处理器芯片和一个内置 2.4GHz 天线 IEEE 802.15.4 的射频器，为数字图像、工业振动监控等高精度、高频率的无线传感器网络应用提供了一个高性能平台。它是无线传感器市场的新一代产品，其无线模块将非常适合于那些支持低功耗、长期工作的高性能传感器节点，并能延长这类节点的使用寿命。

此外，英特尔公司开发出了用于家庭护理的无线传感器网络系统，并于 2004 年下半年开始试用。该系统是作为应对老龄化社会技术项目的一个环节开发的。根据演示，试制系统通过在鞋、家具以及家用电器中嵌入半导体传感器，帮助老年人、阿尔茨海默氏病患者以及残障人士的家庭生活。该系统利用无线通信将各传感器联网，可高效传递必要的信息，从而方便病人接受护理，还可以减轻护理人员的负担。

值得一提的是，基于 IEEE 802.15.4 标准[8]，ZigBee 联盟于 2005 年 3 月发布了 ZigBee 1.0 版[9]，它是一种供廉价固定、便携或移动设备使用的，极低复杂度、成本和功耗的低速率无线连接技术，其数据传输可靠性高、网络容量大、时延较小。

4.2.3.3　学术界研究进展

国外的一些著名大学如加州大学洛杉矶分校、康奈尔大学、麻省理工学院和加州大学伯克利分校等也先后开展了传感网络方面的研究工作，其中以下几项研究值得关注。

加州大学洛杉矶分校 UCLA 在生态监控方面，研究了小气候传感器和视频传感网络技术，包括通过有限的传感器节点和简单且易于测试的通信软件，进行长时间数据收集的应用系统，及其自动分类实时的远端图像数据的收集和嵌入式网络感知技术等。另外，还研究了移动感知平台的生态应用系统、无线传感器中的自适应通信、农业和生态应用中的视频成像节点的部署等内容。在地震监控和响应结构方面，研究了数据通信控制器和网络时间同步、实时地震监控和深埋的下的传感器可靠部署、宽带地震网络、连续实验和结构模型、结构检测的无线地震监控网络。在污染传输监控方面，研究了实验室污染源估计，包括开发提取污染源区域特征的软硬件系统。其实验室岩石影响评估、传输媒介中沙漠土壤物理模型和相关数据获取系统中，初步实现了水渗透和土壤潮湿分布的传感器错误控制、定位传感网络错误算法，并在信息传输中最小化这些错误。

加州大学伯克利分校 UCB 实施了 WINS 项目，项目包括网络嵌入系统技术研究（Network Embed System Technology，NEST），为网络嵌入系统开发了一系列的软硬件实验平台，包括在小型传感器上运行的 TinyOS 操作系统、TOSSIM 模拟器、数据查询系统 TinyDB 以及在 TinyOS 上运行的编译器 NesC，用于传感网络的定位系统 Calamari 链路层加密算法 TinySEC 等。该项目还包括 Sensor Webs、Smart Dust、Pico Radio 等部分。

麻省理工学院 MIT 研究了传感网络和数据流管理系统集成框架和集成两者技术的查询优化技术等，并且获得了 2005 年的 NSF 的资助；在 DARPA 的支持下，研究了用于无线传感网络的中间件技术，大型传感网络可扩展算法，软件应用的灵活性，利用无线和超声波提供定位服务的方法等。此外，还研究了无线传感网络节约能量的拥塞控制、传感网和移动装置网的分布算法和基于知识的信号处理技术等。

对无线传感网络的研究与开发是目前信息领域的一个热点，学术界和产业界对它的学术价值和应用前景非常瞩目。从研究现状来看，无线传感网络的研究历史不长，但发展很快。从 2000 年起，国际上开始出现少量有关无线传感网络研究成果的报道，近年来反映无线传感网络研究各个层面成果的论文逐步增多。传感网络成为国际上近期网络研究的热点之一。ACM 第一届嵌入式传感网络系统的会议于 2004 年 11 方在美国洛杉矶召开，欧洲的第一届专业传感网络的会议也于 2005 年 1 月在德国柏林召开。从国外的研究现状来看，整体的研究成果仍处于原型和小规模试验阶段，与实际应用需求还有一定距离。

在无线传感器网络专题年会、通信和控制类国际会议有关传感器网络部分方面，也均有所增加，如传感网络中的信息处理 IPSN 年度研讨会、无线传感网络欧洲研讨会、传感网络的协议与应用 SNPA 年度研讨会、无线传感网络与应用（无线传感器网络 A）年度研讨会；全球智能与控制 WCICA 双年会等。

4.3.3　无线传感器网络国内研究进展

我国也十分重视无线传感器网络的研究，但相关研究仍处于起步和跟踪阶段。目前取得的成果和研究计划如下。

“十五”期间，中科院组织全院近 20 家研究所开展联合攻关，在基础研究方面，提出

的一系列算法、体系，特别是随机布设传感网、MESH(网状网)传感网、残缺受限分布式任务分配、传感网盲源分离、协同融合、目标跟踪、目标定位等；在重要传感器件方面，自主开发 MEMS(微机电系统)振动传感器、MEMS 声响传感器、MEMS 红外传感器、光纤传感器、声阵列传感器，形成了以 MEMS 传感器为主、复合多信息探测的小型化传感器系列。目前，7 种器件有明确的应用方向，两种器件批量供货，确立了中科院 MEMS 技术水平国内领先地位。在系统层面，研制出了 5 个系列 9 种传感网端机、4 个系列基站等原型样机，在低功耗、微型化等方面研究取得突破。在专用网络研究方面取得重大突破，利用研制的传感网设备可组成多种类型的传感网络，并成功实现了各种无线传感网络与公共网络、卫星网络的加密互联。同时，研制完成了无线传感网核心协议芯片。目前，部分产品已在上海智能交通、嘉兴水运智能交通、浦东机场安全系统等多个领域进行示范应用。

《中国未来 20 年技术预见研究》提出的 157 个技术课题中有 7 项直接涉及无线传感器网络。2002 年以来，国家自然科学基金和其他团体陆续资助无线传感器网络相关技术研究，取得了一些成果。图 4.9 为 2003 年至 2007 年，国家自然科学基金(CSNF)资助无线传感器网络研究的项目数量及资助金额统计[①]。

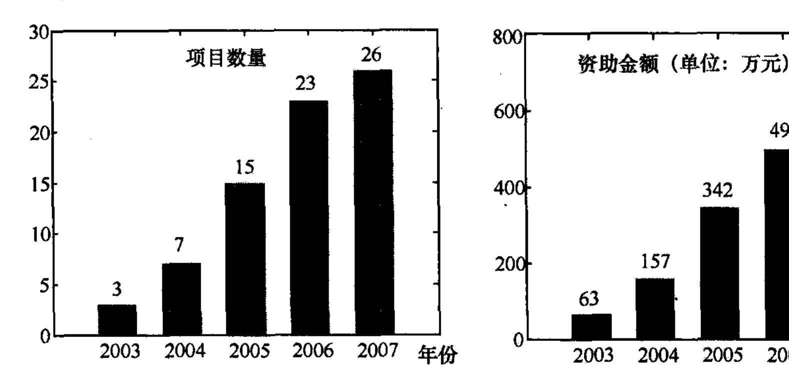


图 4.9　CNSF 资助无线传感器网络研究的项目数量及资助金额统计

2006 年初发布的《国家中长期科学和技术发展规划纲要(2006—2020)》为信息技术确定了 3 个前沿方向，其中，传感器网络与智能信息处理和自组织网络技术两个方向与无线传感器网络研究直接相关。重点开发多种新型传感器及先进条码自动识别、射频标签、基于多种传感信息的智能化信息处理技术，发展低成本的传感器网络和实时信息处理系统，提供更方便、功能更强大的信息服务平台和环境。

2006 年国家自然科学基金重点项目“月球探测系统的建模、传感、导航和控制基础理论及关键技术研究”于 2006 年 1 月启动，为期 4 年。其中，关于在月球探测车月面导航技术方面，在传统的陀螺、视觉和激光导航的基础上，提出了基于无线传感器网络的月球探测车传感、导航、定位方法，为月球探测车消除定位和导航的积累误差以及动态构建月面环境地图与自主路标设置提供了新的方法。

2006 年 11 月，由香港科技大学倪明选教授担任首席科学家的国家 973 项目“无线传感网络的基础理论及关键技术研究”正式启动。该项目集合了上海交通大学、中国科学

① 统计数据来源于国家自然科学基金网站 www. nsfc. gov. cn。

技术大学、中国科学院计算技术研究所、哈尔滨工业大学、南京大学、浙江大学等 7 家研究机构，并在上海交通大学成立了 973 无线传感器网络联合实验室。旨在以煤矿监测、水环境检测、上海世博会安全监控等重大应用需求为牵引，以解决“低耗自组、异构互联和泛在协同的复杂系统及资源优化的自组织网络”问题为核心，从发展新型无线传感网络产业的角度，研究新一代无线传感网络基础理论与关键技术。

2007 年 10 月份，以中科院上海微系统与信息技术研究所为总体单位，并联合上海市多家高校、研究所共同承担的“无线传感器网络关键技术攻关及其在道路交通中的应用示范研究”项目通过验收。该项目建立了无线传感网的仿真、测试、环境模拟平台和交通信息采集综合测试实验外场，填补了城市低等级公路、城郊区域道路的道路信息化空白。

在产业化方面，宁波中科取得一些进展，开发了 GAINS 系列节点，包括 miniGAINS、GAINS3 和 GAINSZ 等。中国无线传感网产业发展联盟也于 2007 年 11 月成立，标志着中国无线传感网技术正式进入产业化应用阶段。

在学术研究方面，中国计算机学会为了推动无线传感器网络的研究，成立了无线传感器网络专业委员会，并于 2007 年 9 月召开了第一届中国传感器网络学术会议。《软件学报》也专门开辟专刊，介绍无线传感器网络最新研究进展。

虽然我国众多高校和研究机构都陆续投入大量人力和财力开展无线传感器网络的研究，但与国外相比，无论是理论研究还是工程实践都有一定的差距。突出表现在，原创性的理论研究较少；理论研究成果难以应用到实际系统中，与实际工程需求尚有一定距离；实际网络平台的规模、成本及可靠性仍不能满足工程需求。

此外，由于军事领域的应用对网络的可靠性、抗毁性及安全性等有更为苛刻的要求，在军用领域无线传感器网络的研究则显得相对滞后。

无线传感网络在新一代网络中具有关键性，甚至决定性的角色，作为一种新的计算模式，推动科技发展和社会进步，已成为国际竞争的焦点和制高点，关系到国家政治、经济、社会安全。发展我国具有自主知识产权的无线传感器网络技术，对我国可持续发展、生态环境和水资源监测、提高煤矿安全、改善井下作业环境、2010 年上海世博会安保等方面，乃至对于我国在 21 世纪提高国际战略的位都具有至关重要的意义。

4.4 无线传感器网络研究新动态及发展趋势

无线传感器网络是一个十分活跃的研究领域，最近也出现了一些新的研究动向，主要体现在面向服务的无线传感器网络应用、无线传感器网格计算和面向无线传感器网络的软件工程几方面。

(1)面向服务的无线传感器网络应用。无线传感器网络具有面向应用领域的特点，对监测数据的收集、预处理，在很多情况下只是为应用提供了必要的基础数据。传感器网络需要与其他系统(如因特网)互联以满足用户复杂的信息处理需求。作为一种网络环境下的新型软件构件，以 Web Service 为代表的服务为封装无线传感器网络中的异构资源提供了新途径。目前，已有研究人员在考虑将两者结合起来构造新型无线传感器网络应用和中间件[10]。其中，如何在资源十分有限的无线传感器网络里实现基于 XML、SOAP 等的服务是一个十分具有挑战性的问题。

(2)无线传感器网格。作为下一代网络技术,网格致力于分布式环境下异构资源的协同共享。无线传感器网络面临着许多与网格相似的问题,如异构传感器的协同使用、海量异构数据的采集处理与共享、分布式环境下的应用协同、对动态运行环境的适应及系统自身的自组织等。网格技术的采用将有助于上述问题的解决,并可以增强无线传感器网络的计算能力。目前,波士顿大学等已经开始了这方面的研究[10]。

(3)面向无线传感器网络的软件工程。无线传感器网络在系统自组织、感知任务协同及节省能源等方面的要求给无线传感器网络应用的构造带来了新挑战。例如,传统无线/有线网络环境采用的客户端—服务器计算模式,已经不能适应自组织无线传感器网络拓扑结构动态变化及任务协同的需要。为此,需要研究新的软件参考结构、开发工具、测试工具和开发方法。另外,对于无线传感器网络中传感器软件、节点软件及网络应用的部署、维护也需要新的工具支持。目前,瑞士苏黎世联邦工学院、美国南加州大学和德国罗斯托克大学等已经开始了这方面的研究[11]。

无线传感器网络技术的发展趋势主要有以下4个方面:

(1)灵活、自适应的网络协议体系结构。无线传感器网络广泛的应用于军事、环境、医疗、家庭、工业等领域。其网络协议、算法的设计和实现与具体的应用场景有着紧密的关联。在环境监测中,需要使用静止、低速的无线传感器网络;在军事应用中,需要使用移动的、实时性强的无线传感器网络;在智能交通里,需要将RFID技术和无线传感器网络技术融合起来使用。这些面向不同应用背景的无线传感器网络所使用的路由机制、数据传输模式、实时性要求以及组网机制等都有着很大的差异,因而网络性能各有不同。目前,无线传感器网络研究中所提出的各种网络协议都是基于某种特定的应用而提出的,这给无线传感器网络的通用化设计和使用带来了巨大的困难。因此,如何设计"功能可裁减、自主灵活、可重构和适应于不同应用需求"的无线传感器网络协议体系结构,将是未来无线传感器网络研究领域的一个非常重要、非常具有挑战性的发展方向。

(2)跨层设计。无线传感器网络具有层次化的体系结构与拓扑结构,因此在具体设计时也大都基于分层的思路进行。这种方式保证系统具有很好的层次性和伸缩性,易于修改和重用。但各层的设计相互独立且具有一定局限性,因而各层的优化设计并不能保证整个网络的设计最优。因此,一些研究者提出了跨层设计的概念,即不同层间可以共享信息并实现跨层操作。跨层设计的目标就是实现逻辑上并不相邻的协议层之间的互动设计与性能平衡。对无线传感器网络而言,能量管理机制、低功耗设计等在各层设计中都有所体现,但要使整个网络的节能效果达到最优,还应采用跨层设计思想。例如,将物理层协议与MAC协议相结合、MAC协议与路由协议相结合进行跨层设计可以有效节省能量,延长网络寿命。同样,传感器网络能量管理和低功耗也必须结合实际进行跨层设计。此外,时间同步和节点定位也可采用跨层设计,这样能够使节点直接获取物理层信息,有效避免信息本地处理带来的误差,获得较为准确的信息。尽管跨层优化算法能够极大的提高系统的效率,但这种方法影响了系统层次化与模块化,增加了系统设计的复杂度。

(3)与现有网络的融合。为了大范围使用传感器网络的数据,扩展无线传感器网络的使用效能,实现基于传感器网络的新应用,与现有网络的融合十分必要。它可以同互联网、移动通信网进行融合,一方面,使无线传感器网络得以借助其传递信息;另一方面,这

两种网络可以利用传感信息实现应用的创新。

另外，将无线传感器网络作为传感与信息采集的基础设施融合进网格体系，构建一种全新的基于无线传感器网络的网格体系——无线传感器网格。传感器网络专注于探测和收集环境信息；复杂的数据处理和存储等服务则交给网格来完成，无线传感器网格的实现将能够为大型的军事应用、科研试验、工农业生产和商业活动等领域提供一个集数据感知、密集处理和海量存储于一体的强大的操作平台[12]。

(4)网络标准的制定。IEEE 于 2002 年开始研究制定两个无线传感器网络的相关标准。IEEE802. 15. 4 是低速无线个域网标准，其定位于物理层标准，主要涵盖物理层和 MAC 层标准；IEEE1451 是关于无线智能变换器的接口标准，其定位于面向互操作的应用层接口标准，而在物理层和应用层中间的大量通信协议没有相应的标准。

目前，ZigBee 正在进行网络层协议和 API 的标准化工作，它的基础是 IEEE802. 15. 4 技术标准，此外，ZigBee 联盟还开发了安全层，以保证这种便携设备不会外泄其标识，远距离传输不会被其他节点获得。

参考文献

[1] Federal Agencies Need to Improve Controls over Wireless Networks[R]. United States Government Accountability Office, 2005, 5.

[2] Akyildiz I F, Su W, Sankarasubramaniam Y, etc. Survey on Sensor Networks[J]. IEEE Communications Magazine, 2002, 40(8):102 - 114.

[3] Intanagonwiwat C, Govindan R, Estrin D. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks[A]. ACM/IEEE International Conference on Mobile Computing and Networks (MobiCom2000) [C]. Boston Massachusetts, 2000, 8.

[4] Jie Zhang, Bo Jing, Zonglin Zhang. Research on Spatial - Temporal Information Fusion System for Sensor Networks Node Cluster[A]. the 6th World Congress on Intelligent Control Automation (WCICA06)[C]. IEEE Robotics and Automation Society, 2006. 4:3188 - 3193.

[5] Jinglun Shi, Weiping Liu. A Service - oriented Model for Wireless Sensor Networks with Internet. Proceedings of the Fifth International Conference on Computer and Information Technology, 2005: 1045 - 1049.

[6] Dimitrios Lymberopoulos, Andreas Savvides. A Wireless Sensor Node Architecture for Exploring Distributed Sensor Network Applications[R]. DRAFT - Work in Progress, 2005.

[7] Chen Shuai, Zhong Xianxin, Li Xiao - yi, etc. Pervasive Reconfigurabl e Sensor Network Instrument [A]. 3rd International Symposium on Instrumentation Science and Technology (ISIST) [C]. 2004, 11:1248 - 1252.

[8] Estrin D. Embedded networked sensing research: Emerging systems challenges. In NSF Workshop on Distributed Communications and Signal Processing. Northwestern University, December 2002.

[9] Estrin D, Govindan R, Heidemann J, etc. Next century challenges: Scalable Coordination in Sensor Networks. In Proc. ACM/IEEE MobiCom, 1999, 263 - 270.

[10] Rimon Barr, Zygmunt J Haas , Robbert vanRenesse. JiST: An Efficient Approach to Simulation Using Virtual Machines. SoftwarePractice and Experience, 35(6), 2005: 539 - 576.

[11] Levis P, Lee N, Welsh M, etc. TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications. Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 2003:126 - 137.

[12] Yanyuejie, Wangshu, Zhaohao. MPAS: a connecting platform for integrating wireless sensor network with grid[C]. In proceeding of 11th Asia - Pacific conference on communication, 2005:1000 - 1004.

第5章　无线传感器网络体系结构与拓扑结构

无线传感器网络的构建是一个庞大的系统工程，它以应用为目标，涉及到的研究内容和需要解决的问题在各个层面上都很多，而体系结构是开展无线传感器网络研究的首要内容。网络体系结构的主要功能是组网与通信，它是无线传感器网络得以正常工作的基础。

在无线传感器网络中，提高能量利用效率，研究和开发有效的、实用的无线传感器网络拓扑结构，开发专用的通信协议和路由算法，设计有效的策略，延长网络的生命周期都成为目前无线传感器网络研究的核心课题。

无线传感器节点根据一定协议和网络拓扑结构生成无线传感器网络，并通过相互协作完成复杂的测量任务。无线传感器网络覆盖与连通问题是无线传感器网络研究的基本问题与重要问题之一。无线传感器网络的覆盖面积是用于衡量无线传感器网络测量性能的重要指标，该指标与无线传感器节点的类型及应用目标有关。为了保证无线传感器网络的测量有效性，通常要求监测范围内的任意一点都至少处于一个无线传感器节点的测量范围内。

本章将对无线传感器网络的体系结构、网络拓扑结构与控制、网络覆盖与连通等问题进行详细的阐述。

5.1　无线传感器网络体系结构

5.1.1　应用需求与应用模式

5.1.1.1　应用需求

无线传感器网络是面向应用的网络，它的体系结构设计是依据具体应用场景而构建的。因此，不同的应用场景存在不同的网络应用需求，主要体现在以下几个方面：

(1)能量有效性需求。智能监测的无线传感器网络需要长期在无人值守或半无人值守的状态下工作，网络节点由于电源能量的原因会失效或废弃，电源能量约束是阻碍应用的严重问题。因此，降低网络节点的平均能耗，以求最大化网络生命周期，是最迫切的应用需求。

(2)智能化工作模式需求。系统需要感知目标或对象的状态变化，通过节点间协同工作来产生需要的输出，而系统规模大、资源严格受限和物理世界密切相关等特点使无线传感器网络需要一种新的智能化工作模式。

(3)网络动态拓扑需求。无线传感器网络系统中，节点间以一种对等、多跳的方式通信，节点都兼备数据采集和无线路由功能，网络中不存在中心控制点，用户节点之间的地位是平等的。鉴于新节点加入或已有节点失效所导致的网络拓扑结构变化，需要设计一

种适合无线传感器网络通信特点、低开销、便于维护的拓扑结构,并且路由协议必须能感知由于各种原因而导致的网络拓扑结构变化。

(4)低成本、通用性需求。为了达到降低成本的目的,需要设计计算、存储能力要求较低的简单网络系统和通信协议,使网络中的节点能够检测到其他节点的存在并共同组成一个具有一定功能和结构的网络系统,并且应该可以满足类似应用需求下的正常工作,因此网络及其节点具有一定通用性的设计需要。

5.1.1.2 应用模式

无线传感器网络的典型应用模式可分为两类:一类是传感节点监测环境状态的变化或事件的发生,并通过簇头节点和 Sink 节点上传给用户;另一类是用户发布命令通过 Sink 节点和簇头节点给某一区域的传感节点,传感节点执行命令并反馈相应的监测数据。

与之对应,通信模式也主要有两种:一种是传感节点将采集到的数据传输到用户,即多对一(Many-to-One)通信;另一种是用户向区域内的传感节点发送命令,即一对多(One-to-Many)通信。前一种通信模式数据量大,后一种则相对较小。

具体而言,传感网络的主要特性是网络中所有网络节点协作完成一个共同的任务。为满足不同硬件的需要,将复杂应用目标分解为不同的任务,并将这些任务分配给层次化网络中的相应硬件,分配的目标是使不同任务需求和不同节点能力相匹配。

传感器网络中各种应用目标都包含不同的监测任务,并均存在3个最基本的任务类型:网络感知、信息处理和网络通信。网络感知是从监测目标获取物理信息的过程,不同传感器节点获取的数据可以在网络内或网络外得到处理,以获取对监测对象更确切的认识,通信过程使多传感器之间的协作式信号和数据处理及处理结果的传递成为可能。

1. 网络感知

网络感知是采用不同类型的传感器节点从监测目标获取物理信息,所有信号从其发生源处开始衰减。因此,信噪比(Signal-to-Noise Ratio,SNR)将随着通信距离的增加而降低。SNR 是决定信号处理(如滤波、计算和估计)质量的基本因素。将传感器节点尽可能密集地部署于目标周围,这样能够提高感知结果的质量。另外,采用数据融合还可以提高感知数据的置信度。

不同的感知任务具有不同的硬件需求,包括采样率、采样精度等方面。在采样率较低的应用中,如环境监测,周围的温度可能变化得很慢,采样率则可以低至每采样一次。为使传感器的部署密度高且接近被测目标,可采用自带能源的微型节点。微型节点比大型节点的能源利用率更高,能够进一步延长网络寿命。而在一些感知任务对于 CPU 和内存资源的需求较高的应用中,感知任务需求超出小型节点的能力时,如识别鸟类叫声的应用中,声音采样频率需要达到22KHz,将感知任务分配给大型节点。

2. 信息处理

信息处理是无线传感器网络的基本任务。信息处理过程通常需要综合多个局部相邻传感器节点的输出,因此是一个协作式信号和数据处理过程,即数据融合或数据聚集。协作式处理具有两个优点:一是通过综合多传感器输出,处理结果具有更高的可靠性和精确度;二是通过发送整合后的数据可以有效降低能耗。微型节点的计算能力通常有限,只适合简单的处理过程。因此,微型节点所能处理的数据融合任务包括计算不同传感器结果的平均值、最小值或最大值等。在层次型结构的网络处理中,微型节点通常充当前端采集

节点的角色,为后继处理过程完成数据的预处理。

对于采集信号的处理,微型节点通过获取数据中最重要的特征值来实现数据融合,降低数据的冗余度,这样的预处理过程在很大程度上减少了大型节点的计算负担和节点之间的通信负担,大型节点则应该主要完成需要进行复杂计算的处理任务,这样有效节约了节点系统和网络系统的能量。这种信息处理方式与将所有原始数据都传递到基站的方式相比,网内处理过程通过减少通信花费节约了大量能源。

3. 网络通信

网络通信是传感器网络中最复杂的任务。与传统的计算机网络一样,通信依照不同层分为几个子任务。通常的分解过程涉及 MAC 层和网络层。网络通信使协作式处理和传感器网络交互成为可能。在分簇型层次化网络中,如果簇中包含大型节点,则通常将其选为簇头节点。无论节点尺寸多大,都必须采用相同的通信模块和低级通信协议。LEACH 是一个很好的实例:网络中各簇之间采用 TDMA 协议实现通信,簇内节点只将其数据传递给簇头节点,而簇头节点采用长距离无线通信将整合后的数据传递到 Sink 节点或基站中;簇头节点的角色在簇成员中轮换以平衡网络系统能耗。

在通信过程中,可能大部分通信负担处于一部分节点中。如果簇能采用对等(Peer to Peer,P2P)通信的方法,则簇成员之间只需要完成簇内的通信路由,而簇头节点则需要完成簇内与簇间的通信路由。任务分解和分配是层次化网络设计的重要内容。适当的任务分配有助于提高感知的可靠性,减少网络花费,以及减少计算、通信过程中的能量消耗,对于剩余资源的利用率也更高。

无线传感器网络的特性对网络体系结构的设计具有直接的影响,这点已得到研究人员及相关领域的广泛证实,这些特点来源于应用需求和技术限制。无线传感器网络的典型应用存在很大差异,既具有共性,如低花费、小尺寸、低能耗、效率高、通用性好、容错性好、自治性、保密性和安全性等,也需要针对应用考虑的相关的技术,如低能耗、低花费的处理器与低花费的存储器技术等。因此,体系结构构建和设计应围绕应用需求、应用模式和技术约束展开,充分体现无线传感器网络自身的特点与优势。

5.1.2　无线传感器网络功能结构、逻辑结构及典型体系结构

5.1.2.1　无线传感器网络的布置

无线传感器网络的应用领域日趋广泛,应用形式日渐丰富。它可根据实际需求,按照合理的体系结构和通信协议进行网络构建,其生成过程分为随机类和固定类两种。固定类的网络构建相对简单,只需将节点按照事先确定的位置放置即可。随机类的生成过程归纳起来主要有以下几步。

第 1 步:网络节点通过机械投放、飞行器空投、炮弹弹射等随机方式进行撒播放置。

第 2 步:撒播后的传感器节点进入到自检测和启动唤醒状态,每个传感器节点会交互组网信号,并记录邻居传感器节点的初始工作情况。

第 3 步:传感器节点会根据监控到周围传感器节点的情况,包括能量剩余、数据冗余、数据路由、信道接入等,从而采用相关的组网算法,按预设方式或规律结合形成网络。

第 4 步:组成网络的传感器节点根据路由算法选择合适的路径进行数据通信。

具体生成过程如图 5.1 所示,图 5.2 为网络节点实际抛撒图。

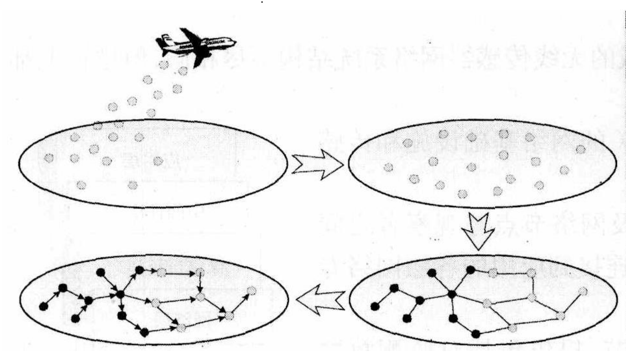


图5.1　无线传感器网络生成过程图

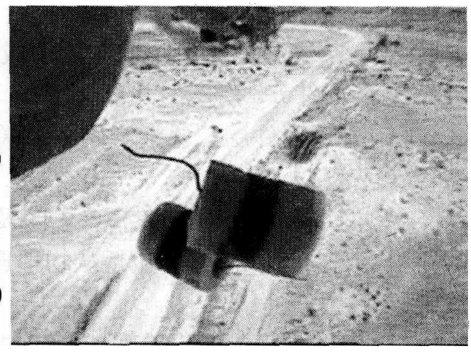


图5.2　网络节点实际抛撒过程

5.1.2.2　无线传感器网络功能结构

无线传感器网络概念化的抽象层面结构模型包括功能结构和逻辑结构。功能结构方面，无论无线传感器网络系统采用哪种拓扑结构，都应该具有以下主要功能：

(1)数据采集与计算。网络节点具有收集与预处理被监测对象数据的能力和数据路由计算的能力。

(2)通信。网络按照一定的数据传输模式，将采集到的数据传递到对被监测对象感兴趣的Sink节点，通信功能由无线通信模块完成。

(3)协同。网络中往往存在大量网络节点，各节点需要相互协同，完成一个大的感知任务。为实现网络的最佳性能，在通道传输处理模式下，网络节点必须同时从传感器中采集、处理、压缩监测数据并传送到网络中，顺序操作是不可行的，即信息存在协同支持的问题。因此，存在两种概念性的方法，一种是将处理器分割成不同的单元，每个单元负责不同的任务；另一种是缩减切换时间。

(4)重配置。根据自然环境、能源、用户需求等变化，整个系统能够对节点重新部署、软件更新、网络拓扑结构变化等提供支持。

(5)安全和保密。每个网络节点需要有足够的安全机制来阻止未经授权的访问、攻击和网络节点的信息故障。要求系统能够安全、可靠地完成数据的采集、传输、处理和存储。此外，还需要一定的保密机制。

(6)设计和用法的多样性。因为每个网络节点尽可能需要小尺寸、低能耗及物理相似性，因此网络节点设计倾向于解决特定的问题。同时，不同传感器节点具有不同的设计要求。因而，传感器节点的设计应在重复使用性、花费和效率间寻找平衡。

(7)兼容性。软件成本在整个系统成本中占据主要地位。通过代码重构或代码变换以重用代码，对于降低网络成本有很大帮助。

(8)低能耗。传感器网络的任务执行能力、使用寿命和网络性能均与能量相关。传感器在不更换电池的情况下能够生存相当长时间也是重要的功能设计内容。

(9)柔性功能的动态调整。这是一个很重要的问题，有两种途径可以提高传感器网络柔性，一是编程，配置可编程处理器，如基于MCU、MPU和DSP平台；二是重构，基于硬件进行软件开发，如基于CPLD和FPGA平台。柔性通常是通过编程或采用特殊的专用集成电路(Application Specific Integrated Circuit, ASIC)和低能耗处理器实现的。

5.1.2.3　无线传感器网络逻辑结构

逻辑结构方面，尽管不同应用领域的无线传感器网络系统结构不尽相同，但逻辑上都大致包含如图 5.3 所示的几部分。

(1) 基础硬件层。包括与网络相关的网络基础设施和传感器等硬件。

(2) 网络层。处理网络节点之间及网络节点与观察者之间的路由、数据传递等问题，包括从物理连接到应用的各层网络专用协议。

(3) 中间件层。封装底层实现细节，提供包括对监测数据的处理、分析、存储、查询和挖掘的接口及与其他类型网络与系统的服务接口，并负责协同任务的调度和安全管理，提供面向应用领域的通用服务。

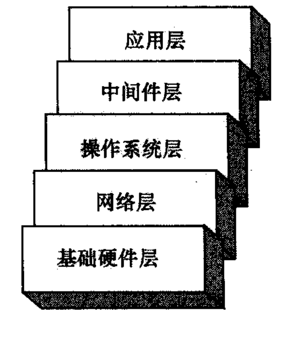


图 5.3　无线传感器网络逻辑结构

(4) 操作系统层。实现物理硬件的抽象，负责管理网络系统资源，实现模块的动态调度和消息管理等。

(5) 应用层。包括面向应用领域、满足用户需求的特定应用，如山洪预警、海洋污染监测、煤矿瓦斯监测、地下探测等。

5.1.2.4　典型网络体系结构

分簇型网络是无线传感器网络的典型网络体系结构，如图 5.4 所示。该网络节点分为 3 类：Sink 节点、簇头节点和传感器节点。Sink 节点担任无线传感器网络和有线网络的网关，监测数据通过 Sink 节点转送到有线网络。簇头节点通过单跳或多跳路由方式与 Sink 节点进行数据通信。传感器节点是固定的或可移动的，它把感知数据向簇头节点传送，并由簇头节点实现簇内感知数据的聚集与融合。

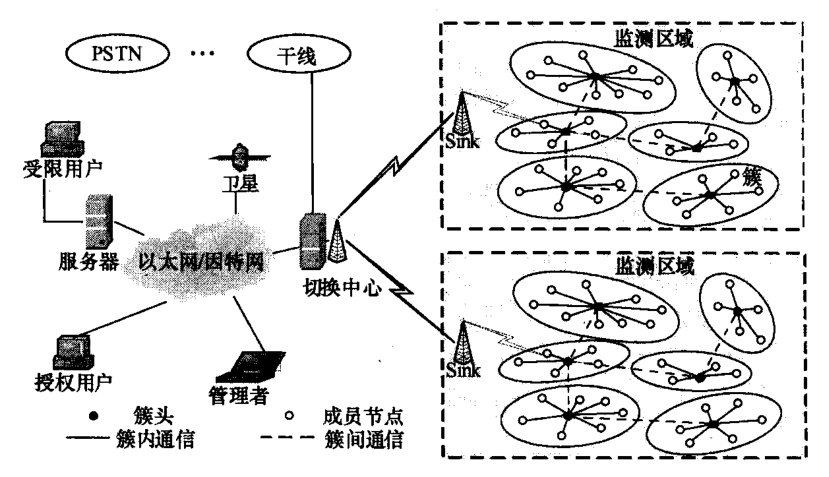


图 5.4　分簇型网络结构

图 5.5 给出了无线传感器网络的又一种典型结构。节点布置结束后，通过预先设计的算法自组织成网络，并通过单跳或多跳中继方式将监测数据传送到 Sink 节点，Sink 节点一方面以同样方式将相关控制信息传送给各网络节点，一方面借助长距离或临时建立的 Sink 链路将整个区域内的数据传送到远程监控或数据处理中心进行集中处理。Sink 链路建立的方式有卫星链路、地面无线基站链路、区域上空无人机链路等。

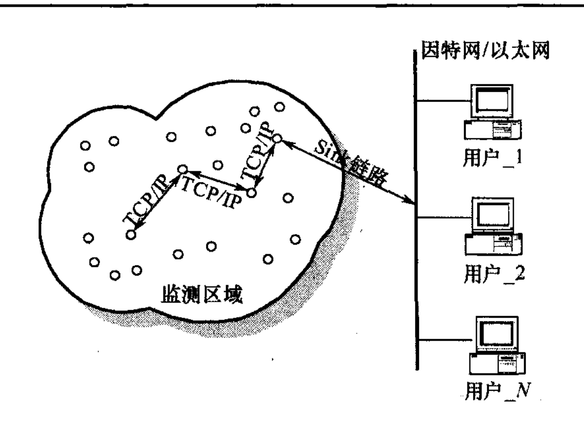


图 5.5　平面多跳网络结构

目前,无线传感器网络广泛借鉴细胞单元型网络结构进行体系结构的构建。所谓细胞单元型网络结构,首先,在一些区域中配置一系列的基站,每个基站周围形成一个细胞单元,并覆盖一定的区域。移动的无线网络节点和其他组件只要在该细胞单元的覆盖范围之内,就可以通过无线方式进行通信。尽管固定的基站需要耗费大部分能量来进行通信,但该结构的通信能力处于中等水平。这种细胞单元型无线网络结构也有一定缺点,主要表现在它必须固定于某个区域中,同时各细胞单元必须经过精心设计以便能够覆盖尽可能多的区域,并实现各细胞单元间的通信。其次,Ad hoc 多跳网络体系结构也是值得借鉴的,但目前并没有证据表明,这种网络体系结构在所有的应用环境中都是最佳的。由于网络体系结构中无线通信模块和数据帧数量的原因,在多跳 Ad hoc 网络体系结构中产生了不对称的现象。事实上,在一些诸如智能建筑或科学实验应用中,网络并不随着空间的改变而改变,通常采用部分固定的节点来搭建网络。这些部分可以与稳定电源供应模块相连,所以无线部分可以采用低功耗通信方式,而且节点有时也可以进入待机状态。

5.1.3　网络节点体系结构

无线传感器网络节点是组成无线传感器网络的基本单位,是构成无线传感器网络的基础平台。每一个传感节点都是由电源、感知部件、嵌入式微处理器、存储器和通信部件等部分构成。节点主要完成信息采集、数据融合、数据传送的功能,电源为传感器提供正常工作所必需的能源,负责节点的驱动,是决定网络生存期的关键因素。感知部件用于感知、获取外界的信息,并将其转换为数字信号,处理部件负责协调节点各部分的工作,如对感知部件获取的信息进行必要的处理、保存,控制感知部件和电源的工作模式等,通信部件负责与其他传感器或观察者的通信。此外,每个节点上还有运行在其上的软件,为传感器提供必要的软件支持,如嵌入式操作系统、嵌入式数据库系统等。因此,节点技术的进步与无线传感器网络的发展有着密切的联系。

节点的设计在不同应用中各不相同,但其基本原则是采用尽量灵敏的传感器、尽量低功耗的器件、尽量节省的信号处理和尽量持久使用的电源。节点中的传感、数据处理、通信及电源各模块技术的进步对节点技术的发展都有着深刻的影响。传感模块由最初的传统的传感器发展到智能传感器,再到后来的网络传感器,进而实现了传感器的信息化。

在目前出现的多种节点设计方案中,各方案的实现原理有一定类似性,只是采用了不

同的微处理器及无线通信协议，如采用自定义无线通信协议、802.11 协议、ZigBee 协议、蓝牙协议以及 UWB 通信方式等。现有的典型的节点有 Berkeley Motes、Sensoria WINS、Berkeley PiconodeS、SmartMesh Dust mote 等。

图 5.6 ~ 图 5.8 为固定类传感器网络节点体系结构，对于非固定类传感器网络簇头节点的体系结构与传感器节点的相同。其中，图 5.6 为传感节点的体系结构，图 5.7 为簇头节点的体系结构，图 5.8 为 Sink 节点的体系结构。

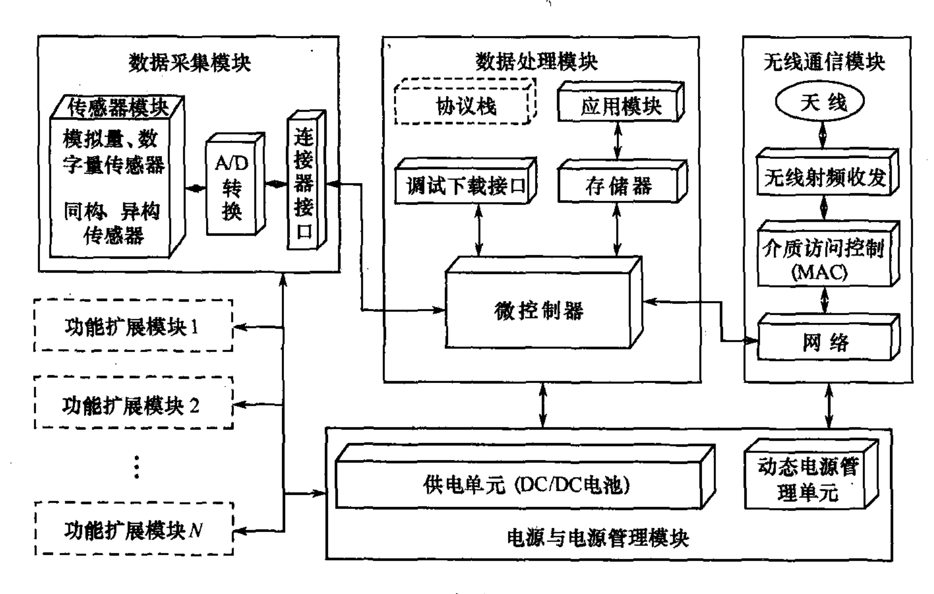


图 5.6　传感节点体系结构

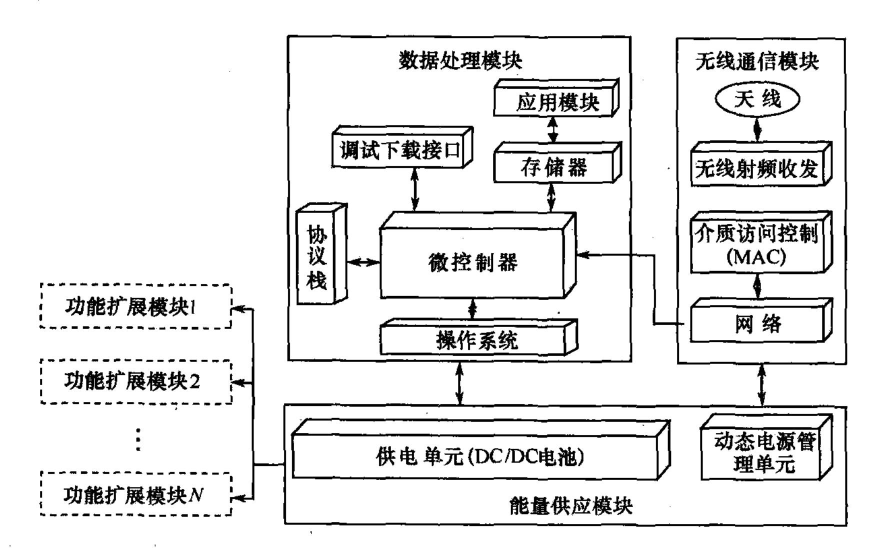


图 5.7　簇头节点体系结构

在节点体系结构中，嵌入式数据处理模块对数据采集模块感知的外界信息进行处理，并控制整个传感器节点的运行。无线通信模块实现网络通信；电源管理模块则对传感器节点的运行提供动态电源管理，报告电源能量剩余情况、存储器存储位置、控制和路由等信息。软件模块包括嵌入式操作系统和应用软件。

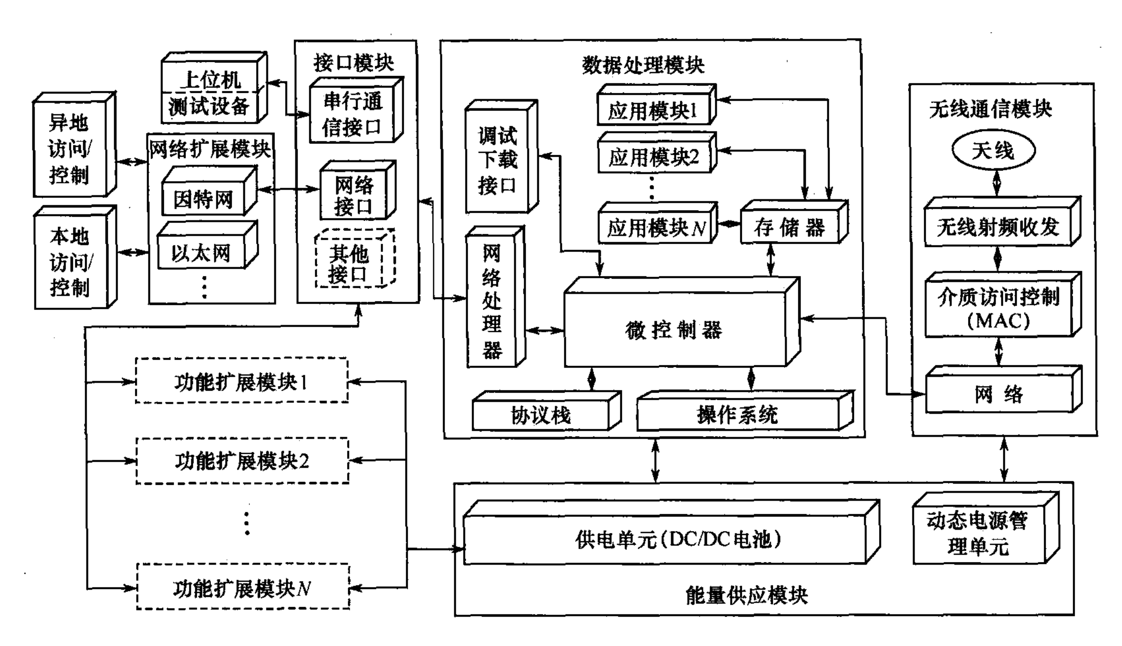


图 5.8　Sink 节点体系结构

传感节点、簇头节点和 Sink 节点体系结构的总体接口框架如图 5.9 所示，在总体框架中，不同的功能模块由相应的功能接口接入，完成不同的任务。

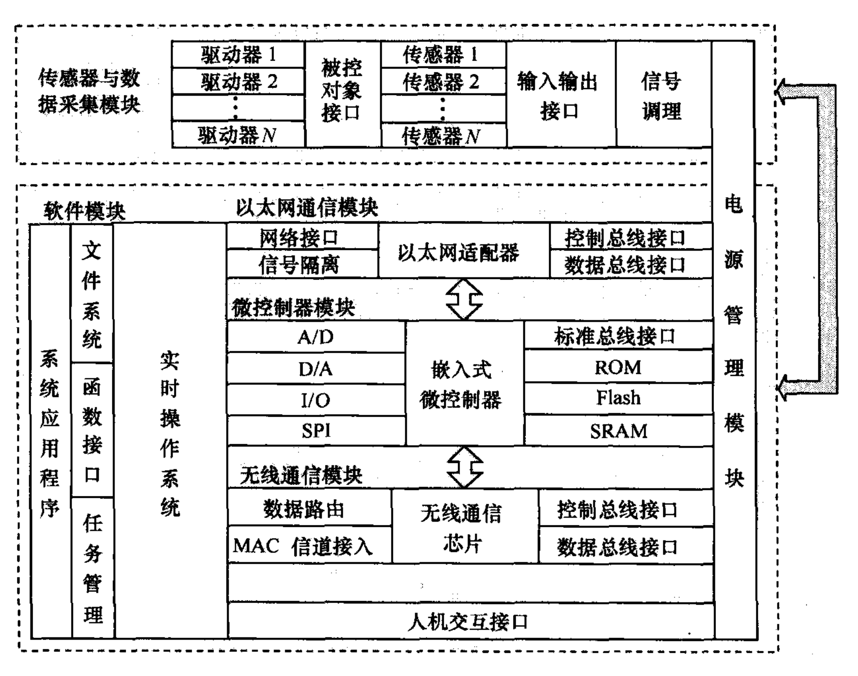


图 5.9　节点体系结构总体接口框架描述

传感器与数据采集模块使各类同构或异构的传感器接入网络，并负责区域内数据采集、转换、调理、放大等。微控制器模块负责控制整个网络节点的组网操作、获取数据的存储与处理。无线通信模块负责与其他网络节点进行无线通信，交换控制信息，完成采集数据调制发送、接收解调。以太网通信模块在 RTOS 统一协调和管理下，通过嵌入式 TCP/

IP 通信协议和网络接口实现数据的以太网双向传输，利用 Sink 节点内嵌的 Web 服务器功能，使用户能够通过用户端标准的浏览器和网络节点进行交互。软件模块主要是针对具体应用实例开发的应用程序，如嵌入式操作系统、嵌入式数据库系统、应用程序等。电源管理模块为网络节点运行提供动态电源管理、报告电源能量剩余信息等。

无线传感器网络实际应用时，网络必须与其他信息设备或其他通信网络进行通信，以满足更大范围资源共享、更灵活资源共享的需求。为实现这个目的，首先，无线传感器网络必须能够与某个移动设备或某种网关交换数据，其中 Sink 节点提供与因特网的物理连接。在物理层和 MAC 层容易实现数据交换给移动设备/网关配备无线传感器网络无线收发机，或无线传感器网络中的部分节点支持标准无线通信技术，如 IEEE 802.11。

Sink 节点的逻辑性使 Sink 节点设计更具挑战性。一种思想是将 Sink 节点视为因特网与传感器网络间的一个简单路由器，这就要求在传感器网络内部使用因特网协议[1]，但一般认为无线传感器网络需要的协议是经过专门优化的，一个简单的路由器不能胜任网关。所以，只能将 Sink 节点设计成一个应用级的网关，即基于应用级信息，Sink 节点必须对其动作做出决策。根据通信发起方，可以大致区分各个待解决的问题。

5.1.4　层次化网络结构

无线传感器网络结构包括平面和层次化两类。平面结构中，所有节点都是对等的，在形态和功能上都是相同的。当节点形成层次化结构时，特定层次的节点针对下一层次的部分节点完成特定任务。虽然平面结构中各节点的完全互换性质具有很多优点，但实际中传感器网络很少采用平面结构。传感器网络一般通过少量的 Sink 节点与一个更通用的网络相连，该网络具有消除冗余数据、复杂计算、数据缓冲和最终的数据传递等功能。传感器网络通常在物理上不是同类的。在应用过程中，由于能量消耗的不平衡，网络可能变成异类网络。网络的定向设置和节点升级同样也可能造成网络的异类化，这是由于给定节点的处理和存储能力将可能发生变化。因此，从成本和能量角度考虑，网络通常最终演变成异类网络。层次化结构对于不平衡分布的资源而言是有利的，它可以对资源进行平衡分配，实现能量的均衡消耗。许多传感网络都建立在层次化结构基础上。

5.1.4.1　层次化网络结构描述

层次化网络的感知、计算和数据传递功能不均匀地分布于节点中。最低层中需要完成所有感知任务，中间层需要完成所有的计算任务，而最高层则需要实现所有的数据传递，如图 5.10 所示。

另外，也可能将某种特殊功能分散到各层中，如在计算的过程中各层将扮演不同角色。在这种情况下，最底层的传感器可能提供简单的带通滤波或模式识别滤波以从噪声中选择出所需要的数据，而高层节点则对从多传感器中获得的已滤波数据进行融合，采用多模型传感器数据对特定时间的监测状态进行描述。

传感器网络的功能分解能反映节点的物理特性，或者也可能是一个简单的逻辑区分。例如，其中具有大范围通信能力的节点子集可以形成一个物理的等级化覆盖网络拓扑逻辑，如图 5.11 所示。另外，网络中的节点子集可以根据对其他节点的服务功能进行逻辑聚类。这些服务可能是数据融合、主流通信和簇头节点路径整合等，逻辑角色分配可能形成一个逻辑型等级化结构，如图 5.12 所示。

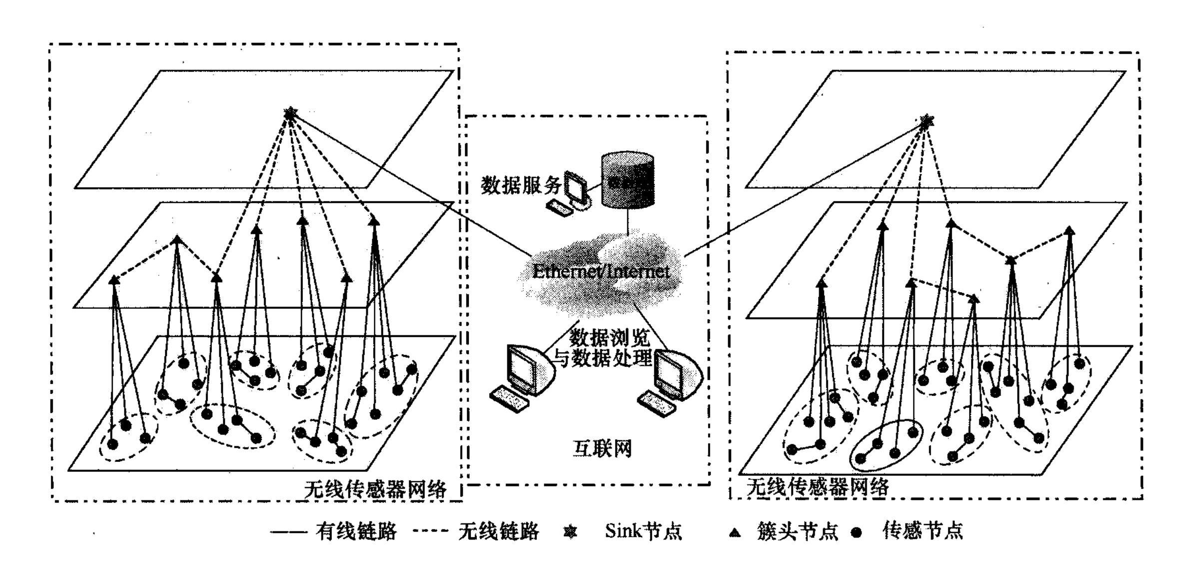


图 5.10　层次结构中的应用功能

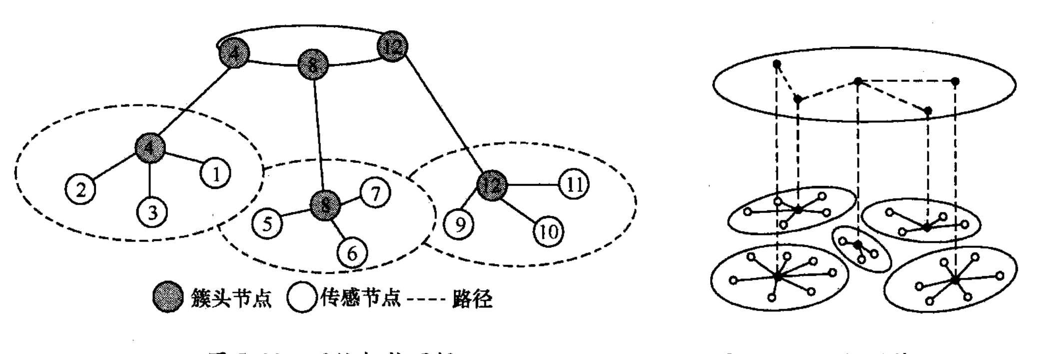


图 5.11　网络拓扑逻辑　　　　图 5.12　逻辑型等级化结构

为使网络消耗更加平衡,逻辑角色可以在网络中循环替换。当某个节点具有更高的计算能力时,计算任务将从计算能力较低的节点中转移至此。如果没有这样的计算服务器,那么每个节点簇中都必须选择出一个节点来完成数据融合的任务。但在一些情况下,只有具有某些特定物理资源的节点能够完成某些特定的工作,如具有 GPS 接收器的节点则需要在位置或时间同步的过程中扮演领导者的角色。为了解层次化结构的重要性,必须首先认识传感网络的 3 个主要特性:花费效率、寿命和可扩展性,这些特性决定了传感器网络是否适用于给定的应用目标。

5.1.4.2　层次化结构的建立

层次化结构的建立可以通过多种机制实现,一些只能构建双层网络,而有些则可以扩展为任意层的网络;有些机制被用于标识和使用具有不同物理特性的组件;其余的一些机制则用于创建小型逻辑节点组以提高网络的可测性。

将网络划分为不同层的简单方法是手动建立网络。网络设计者具体指定哪个节点参与哪一层的工作,及各层节点的组织方法。层次化结构可以通过手动设置路由拓扑逻辑、确定各节点的软件负载或为特定节点提供特定的硬件来实现。该方法常被用于离散型传感网络。在这种情况下,传感器网络中几个密集布置的小型子网络相对布置得较远以形

成一个独立的网络。在每个子网络中，采用短距离通信方式，通信能量消耗少，并采用简单的全向短距离通信天线。传感器簇之间的距离决定了不同簇之间的节点不能相互通信。另外，每个子网络中都包含一个或几个具有长距离通信能力的节点。这些节点包含由更敏感且功能更强大的无线电通信模块或定向天线，这样就可以形成网络的通信主干。

将网络组织为层次化结构可提高网络路由效率。在平面型传感器网络中，路由探寻通常需要将数据帧通过泛洪方式传递到整个网络中。层次化路由包含两种形式：一种形式是查询到达目标节点的路由过程可以根据网络的层次特性发生变化；另一种形式是节点的层次位置与节点地址可以相互编码得到。后一种方法通过引入常变的节点地址简化了路由的探寻过程。

在层次化网络中，路由的探寻可以通过将问题简化为以下两种类型：局部簇内节点的路由和局部簇外节点的路由。如果簇规模较小，则簇内的路由探寻额外花费较低。在很多情况下，假设一定数量的通信区域是可信的。因此，有些时候需要采用花费较高的全局路由探寻方法。层次化结构同样能够在不增加反馈型路由探寻协议延迟的前提下，减少前馈型路由探寻协议的额外花费。各节点包含特有的标识符和逻辑地址，用于指明自身在层次型网络中的位置。由于节点地址指明了层次型网络中的位置，所以数据帧可以直接传递到目标节点而不需要通过反馈型路由探寻方法，也不需要采用有限的路由表。尽管如此，该方法同样需要一定的机制将特有的标识符映射到层次化地址上。

5.1.4.3　层次化网络通信体系结构

无线传感器网络的设计一般都面向应用，网络结构较为简单，但对网络的功能结构却很难在比较详细的级别上给出。为此，基于智能监测的应用需求、网络规模和无线传感器网络的特点，参考开放系统互联模型 OSI 的 7 层体系结构，结合无线传感器网络的组织构成，研究人员提出了一种带协议栈的层次式网络通信体系结构模型，如图 5. 13 所示。

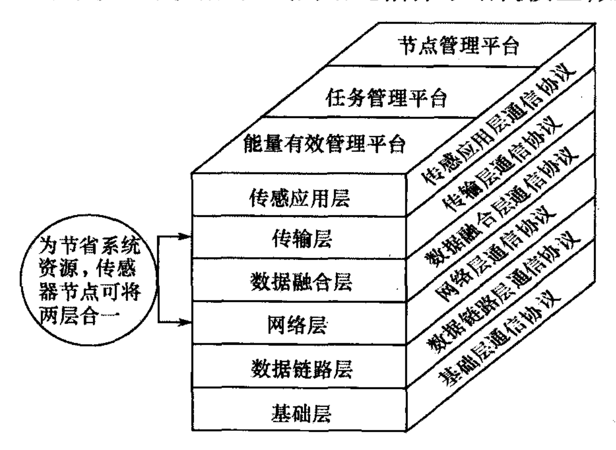


图 5. 13　网络通信体系结构模型

该体系结构分为基础层、数据链路层、网络层、数据融合层、传输层和传感应用层，同时包含了与网络协议有关的能量有效管理平台、任务管理平台和节点管理平台，各层之间通过通信协议链接。

1. 基础层

基础层是体系结构的底层，在实际应用中，是决定无线传感器网络节点体积、成本以

及能耗的关键环节，研究问题的核心是网络节点的硬、软件资源，包括感知器件、嵌入式控制器与存储器、无线通信器件、嵌入式操作系统、基础层协议和物理通信接口等。研究的主要内容包括新型传感器概念、理论和技术的研究；新型传感器材料和新型传感器装置的研究，如化学物质感知材料和装置、生物物质感知材料和装置等；恶劣环境下可操作的传感器技术的研究；把多个传感器计算部件、行为部件集成为一个单集成电路片的微型传感器技术的研究；增强传感器计算能力、感知能力和感知精度的研究；提高传感器健壮性和容错性的研究；缩小传感器体积和重量的研究；传感器电源技术的研究；模拟技术和工具的研究；传感器自校准和自测试技术的研究；传感器制造和封装技术的研究；适应于传感器的嵌入式容错操作系统、嵌入式容错信号处理、嵌入式容错数据库等嵌入式软件系统的研究。基础层的主要功能包括监测感知对象，采集感知信息，无线传输感知信息，初步信息处理以及协调在物理媒体中传输比特流所需的频率选择、载波生成、信号探测、数据加密和调制解调等。

基础层通信协议的设计目标是以能耗和成本为前提，在硬件设计提供调制解调和工作状态切换等功能的基础上，向数据链路层通信协议提供以下功能：

(1)发送节点将数据变换为适合无线信道传输的信道编码及接收节点相反过程的信道解码，这也是该层的关键技术。

(2)原始数据帧传输差错校验。

(3)用于实现链路层中媒体访问控制协议的信道状态检测。

(4)通信起始信号检测。

(5)提供用于减少系统功耗的射频工作状态切换软件接口。

容错控制是无线传感器网络基础层的一个重要内容。一些传感器节点会由于能量的不足、物理损坏或环境等因素而变成无效节点。这些失效的传感器节点不应该影响到整个传感器网络的功能，这就是容错控制的问题。容错控制应该能在某些节点失效的时候还能保持整个传感器网络的工作。运用泊松分布能够为传感器节点建立起容错控制模型，即在一定的时间间隔$(0,t_j)$内，传感器节点未失效的节点可靠性为

$$R_{k_j}(t_j) = \exp(-\lambda_{k_j}t_j) \tag{5.1}$$

式中：λ_k、t_j 分别为节点 k_j 的失效概率和时间长度。

为传感器网络设计的容错控制协议和算法可以根据环境的不同而采取不同的控制能力。如果传感器节点被分布在干扰很少的环境里，那么容错控制要求就可以比较低；如果传感器节点被分布在战场上用来监视和侦察，那么容错控制能力要求就比较高，这是因为感知数据很困难，同时节点也有可能被敌方破坏。总之，容错控制能力水平的高低取决于传感器网络的运用环境，传感器网络的设计必须以此为依据。

2. 数据链路层

数据链路层研究的重点是 MAC 层，MAC 层通信协议将基础层信号转换为可靠的链路，为相互竞争的用户分配信道资源，减少邻居节点广播引起的冲突。考虑到网络环境存在噪声和传感器节点的移动性，其主要功能包括组帧、物理编址、帧检测、流量控制、差错控制、介质访问和数据流的多路技术等，该层协议的目标是向网络层提供可靠支持单播和多播的软件接口，用于建立可靠的点到点或点到多点通信链路。与传统网络 MAC 协议提

高吞吐量和带宽利用率不同,无线传感器网络系统的特点要求 MAC 协议设计必须考虑低能耗、低通信延迟和可扩展性。

著名的无线传感器网络研究人员 Wei Ye 和 Estrin 等人[2]认为:无线传感器网络传输过程中不必要的能量损失主要包括以下几个方面:

(1)数据帧的传输冲突。

(2)由于射频通信媒体造成的冗余接收,即节点会接收目的地址不是自己的数据帧。

(3)节点间控制信息的交互。

(4)即使在不可能有数据传输的时间内,空闲的监听状态依然运行。

因此,MAC 协议的设计的重点是防止通信冲突。目前,各种 MAC 技术的特征可以由控制主体和控制手段这两个因素来区分[3]。

控制主体是指介质访问控制是集中式还是分布式两种方式。集中式中有一个中心站或监控站专门实施介质的访问控制功能,任何工作站必须得到允许才能向网络发送数据;在分布式中,所有的工作站共同完成介质访问控制功能,从而动态地决定发送数据的顺序。在传感器网络中由于网络具有无中心性,所以只能采用分布式控制方式。

控制手段一般分为同步式控制和异步式控制两种方式。同步式控制是指对各个连接分配固定的带宽,这种循环方式的开销太大,对于传感器网络不适用。异步式控制是根据工作站请求的容量分配带宽,主要有循环、预约和竞争 3 种方式。由于循环发送模式功耗过大,为了节省功耗,空闲状态应关闭发射机;预约方案一般用于流式传输的长时间传输,竞争占用方案相对比较适用于局部规模小、数据量不频繁的传感器网络。

在无线自组传感器网络中,MAC 协议必须达到两个目标:第一个目标是建立网络基础。因为成千个传感器节点被随机地分布在某监测区域范围内,MAC 机制必须为数据传输建立通信链路,这种基础结构必须建立起具有单跳形式的通信方式和自组能力的传感器网络。第二个目标是在传感器节点间建立公平、有效的共享通信资源。传感器网络中的 MAC 协议必须满足高效能、移动管理和自恢复策略。虽然已经有很多关于 MANET 的介质访问机制,但是专门为传感器网络设计的 MAC 协议依然是公开研究的热点。

3. 网络层

无线传感器网络属于多跳通信网络,网络层通信(路由)协议的功能是在网络中任意需要通信的两点间建立并维护数据传输路径。主要目标是以网络节能为基础,建立并维护多跳通信中使用的路由表,并根据本地地址信息和路由信息决定是否转发收到的数据帧,同时向应用层提供一个简单易用的软件接口,实现传感节点与用户之间的通信。由于智能监测的无线传感器网络中数据流主要为监测对象的状态信息,因此如何及时有效地将监测信息路由到 Sink 节点是网络层通信协议设计的核心。

网络层主要研究传感器网络通信协议和各种传感器网络技术。一方面通过分析模拟,研究现有通信协议的性能,确定各种现有协议对于传感器网络的可用性及其优缺点。一方面以数据为中心的新通信协议的研究,包括通用能源有效性路由算法的研究、面向应用的能源有效性路由算法的研究、动态传感器网络的路径重构技术的研究等。

此外,还包括可扩展的强壮传感器网络结构的研究,传感器节点的自适应管理和自适应控制技术的研究,资源受限的传感器网络设计策略和性能优化技术的研究,具有局部信息管理能力的能源较低的传感器节点的设计与管理技术的研究,感知数据处理策略的研

究，异构传感器网络技术的研究，传感器网络的安全与认证机制的研究，嵌入与组合系统技术的研究能源有效的介质存取，错误控制和流量管理技术的研究，移动传感器网络技术的研究，传感器网络的自扩展、自适应和自重构技术的研究，传感器网络中传感器节点协作和分组管理技术的研究，传感器网络中传感器节点能源管理技术的研究，传感器网络拓扑结构管理技术的研究，传感器网络中的时间同步技术的研究，数据分发、融合和信息处理技术的研究，仿真技术与仿真系统的研究等。

4. 数据融合层

为了节省网络能源、计算能力和传输能力，在网络层之上增加了数据融合层，以剔除网络中大量存在的冗余数据，降低网络传输的数据比特。数据融合层遵循感知信息“先融合后传输”的原则，通过简单有效的算法，将簇头节点接收到的多源感知信息进行融合（关联、组合、分类、统计），以形成更小、更确定的出口帧转发给下一跳，在最大限度获取感知对象状态信息的同时，有效减少网络能耗，延长网络生命周期。对于只承担感知任务的节点，则融合感知数据和自身的历史数据，对于固定类节点，这部分工作由簇头节点来完成。

数据融合作为对人类信息处理功能的模拟和扩充，是基于多源传感器的观测信息，通过对信息的优化组合得到处理过的有效信息，最终目的是利用多个传感器共同联合操作的优势，提高整个系统的有效性。从广义的信息融合概念出发，融合的主要方法是统计科学和新技术的集成和应用，包括模式识别、决策论、不确定性理论、信号处理、估计理论、最优技术、人工智能和神经网络等。典型方法如下：

（1）加权平均法。最简单直接的方法，该方法将一组传感器提供的冗余信息进行加权平均，结果作为融合结果输出。

（2）投票法。将来自局部的独立决策作为一个有效票看待，融合规则根据具体问题而定，典型的有 AND、OR、K/N 等方法。

（3）贝叶斯融合方法。将各传感器提供的信息以概率值进行定量度量，在融合中依据概率原则进行组合，从而测量不确定性与条件概率表示。

（4）统计决策理论。不同传感器观测到的数据必须经过一个鲁棒综合测试以检验它的一致性，其目的是使互不相同的数据得到最优组合，从而使系统的性能最优而系统的误差最小。

（5）证据融合方法。以证据的信任函数和似然函数构成的信任区间定量度量证据的不确定性，以证据的组合规则实现多个证据下的融合决策。证据融合方法适用于对决策信息的先验概率未知的情况下做出系统的决策。

（6）模糊逻辑方法。将不确定性直接表示在推理过程中。如果采用某种系统化的方法对融合过程中的不确定性进行处理，则可以产生一致性模糊推理。

5. 传感应用层

传感器网络的应用层为用户接入网络提供了接口，同时也提供了对多种服务的支持。由于传感器网络的目的是感知功能，因此传感应用层主要用于将传感节点感知的各种信息转换为网络可用的比特字节流，并根据不同的监测任务，开发和使用不同的应用软件。典型任务包括感知信息的采样处理和发送任务、网络节点状态管理、网络节点任务管理等。

传感应用层是为用户能够在基础层、数据链路层、网络层和数据融合层的基础上开发各种传感器网络应用软件，提供有效的软件开发环境和软件工具。应用层由各种面向应用的软件系统构成。传感应用层的研究主要是各种传感器网络应用系统的开发，包括传感器状态管理、传感器任务管理、传感器感知信息采样处理和发送任务，并传递给下层的网络层。具体应用系统如作战环境侦察与监控系统，战场监测与指挥系统，环境监测系统，交通管理系统，灾难预防系统，危险区域监测系统，有灭绝危险或珍贵动物的跟踪监护系统，民用和工程设施的安全性监测系统，生物医学监测、诊断或治疗系统等。

6. 传输层

传输层按照传感器网络的需求产生数据流，并负责数据流的传输控制，它是保证通信服务的重要部分。当传感器网络需要和因特网或其他外部网络连接的时候，传输层就尤其显得重要。

然而，对于传感器网络传输层的研究不多，目前，基于传输窗口机制的 TCP/IP 协议并不能完全和传感器网络相匹配，必须有一种方法使传感器网络能和别的网络互联。目前，Sink 节点作为无线传感器网络和因特网互联的桥梁，具有 TCP/IP 连接属性，同时 Sink 节点还具备一种传输协议能够处理和传感节点的通信。这样，用户和 Sink 节点之间以 UDP 或 TCP 的方式通过因特网或卫星来通信。另一方面，在 Sink 节点和传感器节点之间纯粹通过传感器网络协议的方式来通信，这是因为每个传感器节点的存储能力有限。

研究传输层协议是项具有挑战性的任务。尤其是硬件的限制，这包括能量和存储容量的限制。因此，传感器网络的节点不能像因特网网络服务那样存储大量的数据。因此，在 Sink 节点处必须分离端到端的通信方式，在传感器网络中采用微型化的 TCP/IP 协议，在因特网或微型网络中采用完整的 TCP/IP 协议。

另外，能量管理、任务管理和节点管理平台分别监视传感器节点中的每个节点的能量、移动和任务。这些管理平台有助于传感器节点调整感知任务和降低总体能量消耗。

(1)能量管理平台。能量有效管理平台管理网络节点如何有效使用能量，在各个协议层都需要考虑节省能量。例如，传感节点在接收数据帧后立刻关闭自己的接收装置，这就避免了接收冗余信息，同样发送数据帧后关闭发送装置。当一个节点的能量比较低的时候，它就会广播给它的相邻节点告知它的能量很低，不能参加路由信息。剩余的能量用于保留感知信息。

(2)任务管理平台。任务管理平台在一个给定的区域内平衡和调度监测任务，为某一特殊区域的传感器节点安排任务和时间计划。同一时间内，某些能量高的节点要承担更多的感知任务，而能量最低的节点进入休眠，因此节点是否执行任务就取决于节点能源级别和任务管理平台对当前状态的判决。这些管理平台都是必须的，只有这样，传感器节点才能结合在一起，低功耗地工作，在节点间共享数据资源。如果没有这些管理平台，传感器节点只能单独各自地工作。如果传感器节点能够协同工作，那么就能提高整个网络的工作效率，可以延长传感器网络的生命周期。

(3)节点管理平台。节点管理平台用来执行节点发现、探测邻居节点状态变迁、移动等任务管理，知道了它们的相邻节点，就能平衡地利用能量和完成任务。同时维护到 Sink 节点的路由，并保证节点获得邻居状态信息，以平衡网络能源消耗和任务管理。

图 5.14 所示的无线传感器网络分层结构模型和 OSI 模型相比，网络协议有所简化。

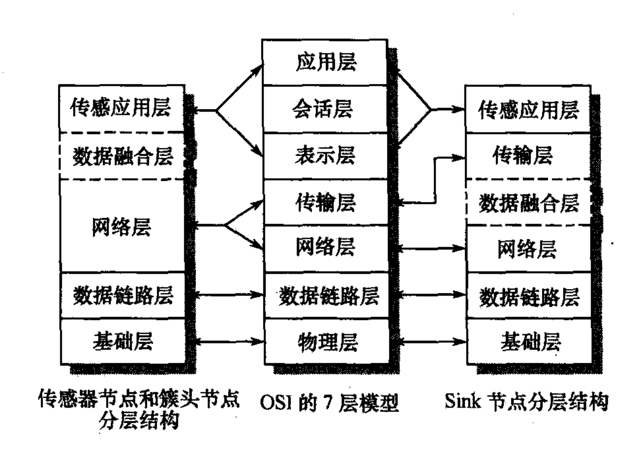


图 5.14　无线传感器网络分层结构模型与 OSI 模型对比

基础层和数据链路层分别与 OSI 模型的物理层和数据链路层对应；在考虑功能的前提下，为节省系统资源，传感器节点可将传输层和网络层合而为一，即传感器节点和簇头节点的网络层等价于传统网络的网络层和传输层，而 Sink 节点作为连接无线传感器网络与因特网的网关节点，保留单独的传输层；在分层结构中，增加了数据融合层，遵循将感知信息先融合后传输的原则，以减少网络中传输的数据比特，实现有限计算能力和能源情况下最大限度地传感任务。模型最上层为传感应用层，对应于 OSI 模型的应用层，主要用于实现通过传感器感知信息并进行预处理。

与 TCP/IP 协议簇相比，主要是增加了数据融合层和基础层，如图 5.15 所示。

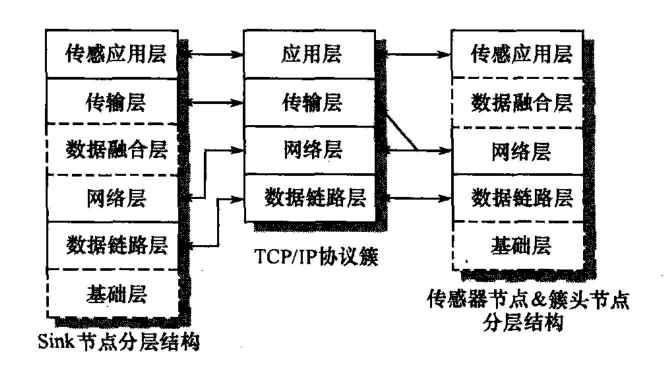


图 5.15　无线传感器网络分层结构与 TCP/IP 协议簇对比

5.1.4.4　层次化结构面临的问题

1. 网络的可扩展性

无线传感器网络必须根据节点的数量调整网络带宽和寿命，但平面型无线传感器网络中的带宽是无法调节的。层次化结构的扩展性研究是很有前景的问题，一种方法是在层次化通信结构中采用单通道，较低层的节点构成了不同的簇，布置在 Sink 节点周围。每个 Sink 节点作为与上层进行交流的桥梁，并实现了簇与簇之间的通信。在这种情况下，网络的容量随簇的数量呈线性增长。在不同网络层采用不同通信通道时，层次化结构中各层的能力和特定层中各簇节点的能力可以独立调节。

2. 结构性价比

应用需求的不同要求采购、布设和维护传感器网络软、硬件的费用可以不同。军用领域中,对传感器网络的投资除了看重价值回报外,更看重的是军事效益;而民用领域的应用中,对传感器网络的投资必须能够获得有价值的回报,即在特定的时间范围内,传感器网络所提供的收益必须大于采购和布设网络的花费。

层次化结构通过最有效地分配资源能够降低传感器网络的花费。感知过程通常需要大量网络节点,且每个网络节点的能耗较低。数据分析通常比感知需要更多的处理和存储资源,由于数据分析带来的延迟与处理器的处理速度成反比,因此,数据分析所需要的最小资源应当取决于可被允许的最大延时。同样,每个节点存储需求与数据分析中的节点数量成反比,同时也受到了算法所能被分割的节点数量的限制。

如果设置了相同类型的硬件,则对于所有的任务,各网络节点都需要分析最少的资源需求。由于所需的网络节点数量可以由所需的传感器覆盖情况所确定,因此,网络的整体花费是个不确定的因素。相反,若采用大量便宜的节点用于感知、少量较贵的节点用于数据分析、定位和时间同步,那么,网络整体花费则可以减少。

3. 网络的生命周期

无论是接近市电还是远离市电,无线传感器节点都无法由市电供电,而必须采用电池供电。由于电池容量增长缓慢,并考虑物理体积和节点成本等因素,因此,延长网络寿命是一件很重要的工作。但应用需求所需要的寿命变化很大,一般的监测应用寿命需求通常为 6 个月至 1 年。

当需要进行复杂计算时,较快处理器的能量效率高于较慢处理器,这是由于它所需的处理时间较少。但对于需要在长时间内进行感知的任务,低功耗节点则具有更高的能源效率。因此,根据不同节点硬件制定的层次化结构有利于延长网络寿命。

5.2　无线传感器网络拓扑结构及控制

无线传感器网络与传统的无线网络(如无线局域网 WLAN 或蜂窝移动网络)有着不同的特点和技术要求。传统的无线网络在高度移动的环境中通过优化路由和资源管理策略最大化带宽的利用率,同时为用户提供一定的服务质量保证。它们的主要目的是提供更好的服务质量 QoS(Quality of Service)和更大的带宽保证,以便能够传输多媒体信息业务。在无线传感器网络中,除了少数节点需要移动以外,大部分节点都是静止的;另外节点能源无法替代,需要尽量节省能量,以便保证网络的连通性和延长网络运行寿命。因此,提高能量利用效率,研究和开发有效的、实用的无线传感器网络拓扑结构,开发专用的通信协议和路由算法,设计有效的策略,延长网络的生命周期都成为目前无线传感器网络研究的核心课题。

5.2.1　拓扑结构分类及拓扑发现

5.2.1.1　拓扑结构分类

无线传感器网络的网络拓扑结构是自组织无线传感器节点的组网技术,有多种形态和组网方式。按组网形态和方式来看,有集中式、分布式和混合式。无线传感器网络的集

中式结构类似移动通信的蜂窝结构,集中管理;无线传感器网络的分布式结构,类似 Ad hoc 网络结构,可自组织网络接入连接,分布管理;无线传感器网络的混合式结构包括集中式和分布式结构的组合。

无线传感器网络的网状式结构,类似 Mesh 网络结构,网状分布连接和管理。如果按照节点功能及结构层次来看,无线传感器网络通常可分为平面网络结构、分级网络结构、混合网络结构以及 Mesh 网络结构。无线传感器节点经多跳转发,通过汇聚节点或网关接入网络,在网络的任务管理节点对感应信息进行管理、分类和处理,再把感应信息送给应用用户使用。研究和开发有效、实用的无线传感器网络拓扑结构,对构建高性能的无线传感器网络十分重要,因为网络的拓扑结构严重制约无线传感器网络通信协议设计的复杂度和性能。下面根据节点功能及结构层次分别予以介绍。

1. 平面网络结构

平面网络结构如图 5.16 所示,它是无线传感器网络中最简单的一种拓扑结构,所有节点为对等结构,具有完全一致的功能特性,也就是说每个节点均包含相同的 MAC、路由、管理和安全等协议。这种网络拓扑结构简单、易维护,具有较好的健壮性,事实上就是一种 Ad hoc 网络结构形式。由于没有中心管理节点,故采用自组织协同算法形成网络,其组网算法较为复杂。

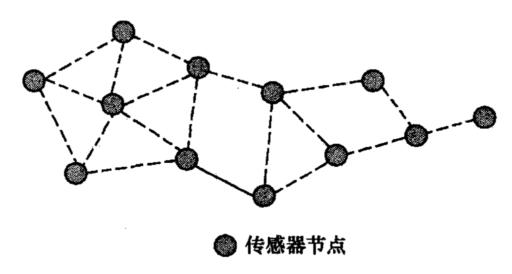


图 5.16　无线传感器网络平面网络结构

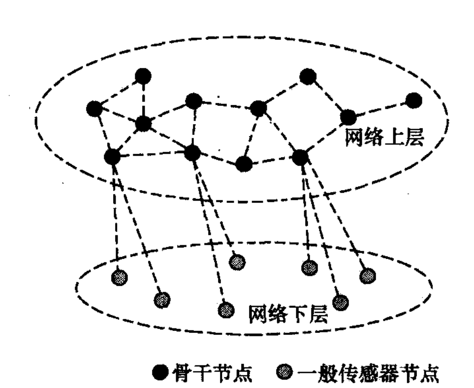
2. 分级网络结构

分级网络结构如图 5.17 所示,也叫层次网络结构。它是无线传感器网络中平面网络结构的一种扩展拓扑结构,网络分为上层和下层两个部分:上层为中心骨干节点;下层为一般传感器节点。具有汇聚功能的骨干节点和一般传感器节点之间采用的是分级网络结构。通常,网络可能存在一个或多个骨干节点,骨干节点之间或一般传感器节点之间采用的是平面网络结构。所有骨干节点为对等结构,骨干节点和一般传感器节点有不同的功能特性,也就是说每个骨干节点均包含相同的 MAC、路由、管理和安全等功能协议,而一般传感器节点可能没有路由、管理及汇聚处理等功能。

这种分级网络通常以簇的形式存在,按功能分为簇头节点和成员节点。分级网络拓扑结构扩展性好,便于集中管理,可以降低系统建设成本,提高网络覆盖率和可靠性,但是集中管理开销大,硬件成本高,一般传感器节点之间可能不能够直接通信。

3. 混合网络结构

混合网络结构如图 5.18 所示,它是无线传感器网络中平面网络结构和分级网络结构的一种混合拓扑结构。网络骨干节点之间及一般传感器节点之间都采用平面网络结构,而网络骨干节点和一般传感器节点之间采用分级网络结构。这种网络拓扑结构和分级网



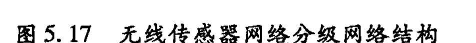


图 5.17　无线传感器网络分级网络结构

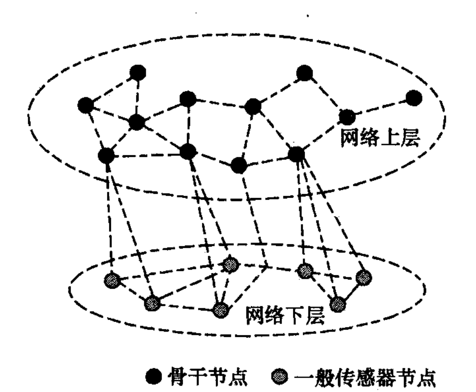


图 5.18　无线传感器网络混合网络结构

络结构不同的是一般传感器节点之间可以直接通信，可不需要通过汇聚骨干节点来转发数据。这种结构同分级网络结构相比较，支持的功能更加强大，但所需硬件成本更高。

4. Mesh 网络结构

Mesh 网络结构是一种新型的无线传感器网络结构，较前面的传统无线网络拓扑结构具有一些结构和技术上的不同。

从结构来看，Mesh 网络是规则分布的网络，不同于完全连接的网络结构，如图 5.19 所示。通常只允许和节点最近的邻居通信，如图 5.20 所示。网络内部的节点一般都是相同的，因此 Mesh 网络也称为对等网。Mesh 网络是构建大规模无线传感器网络的一个很好的结构模型，特别是那些分布在一个地理区域的传感器网络，如人员或车辆安全监控系统。尽管这里反映通信拓扑的是规则结构，然而节点实际的地理分布不必是规则的 Mesh 结构形态。由于通常 Mesh 网络结构节点之间存在多条路由路径，网络对于单点或单个链路故障具有较强的容错能力和鲁棒性。Mesh 网络结构最大的优点就是尽管所有节点都是对等的地位，且具有相同的计算和通信传输功能，但某个节点可被指定为簇头节点，而且可执行额外的功能。一旦簇头节点失效，另外一个节点可以立刻补充并接管原簇头那些额外执行的功能。

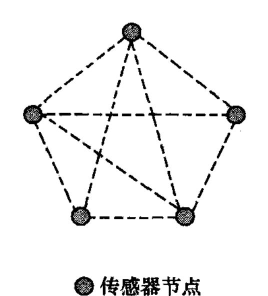


图 5.19　完全连接的网络结构

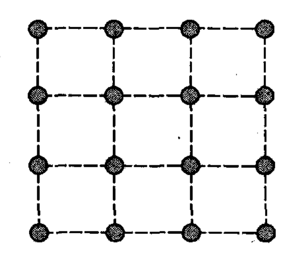


图 5.20　无线传感器网络 Mesh 网络结构

不同的网络结构对路由和 MAC 的性能影响较大。例如，一个 $n \times m$ 的二维 Mesh 网络结构的无线传感器网络拥有 $n \times m$ 条连接链路，每个源节点到目的节点都有多条连接路径。对于完全连接的分布式网络的路由表随着节点数增加而成指数增加，且路由设计复杂度是个 NP-hard 问题。通过限制允许通信的邻居节点数目和通信路径，可以获得一

个具有多项式复杂度的再生流拓扑结构，基于这种结构的流线型协议本质上就是分级的网络结构。如图 5.21 所示，采用分级网络结构技术可使 Mesh 网络路由设计简单得多，由于一些数据处理可以在每个分级的层次里面完成，因而比较适合于无线传感器网络的分布式信号处理和决策。

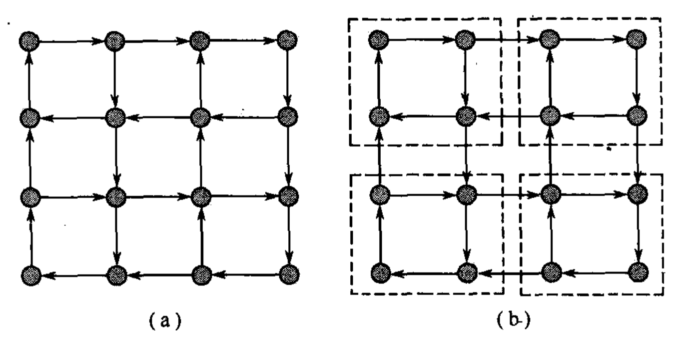


图 5.21　采用分级网络结构技术的 Mesh 网络结构
(a)4×4Mesh 网络；(b)分级分簇网络。

从技术上来看，基于 Mesh 网络结构的无线传感器具有以下特点：

(1)由无线节点构成网络。这种类型的网络节点是由一个传感器或执行器构成且连接到一个双向无线收发器上。数据和控制信号是通过无线通信的方式在网络上传输的，节点可以方便地通过电池来供电。

(2)节点按照 Mesh 拓扑结构部署。图 5.22 所示为一种典型的无线 Mesh 网络拓扑，网内每个节点至少可以和一个其他节点通信，这种方式可以实现比传统的集线式或星型拓扑更好的网络连接性。

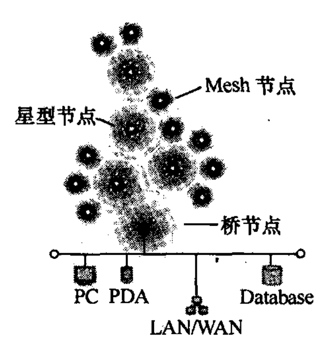


图 5.22　一种典型的无线 Mesh 网络拓扑

除此之外，Mesh 网络结构还具有以下特征：自我形成，即当节点打开电源时，可以自动加入网络；自愈功能，当节点离开网络时，其余节点可以自动重新路由它们的消息或信号到网络外部的节点，以确保存在一条更加可靠的通信路径。

(3)支持多跳路由。来自一个节点的数据在其到达一个主机网关或控制器之前，可以通过多个其余节点转发。在不牺牲当前信道容量的情况下，扩展无线传感器网络的覆盖范围是无线传感器网络设计和部署的一个重要目标之一。通过 Mesh 方式的网络连接，只需短距离的通信链路，经受较少的干扰，因而可以为网络提供较高的吞吐率及较高的频谱复用效率。

(4)功耗限制和移动性取决于节点类型及应用的特点。通常，基站或汇聚节点移动性较低，感应节点可能移动性较高。基站通常不受电源限制，而感应节点通常由电池供电。

(5)存在多种网络接入方式。如图 5.22 所示，可以通过星型、Mesh 等节点方式和其他网络集成。

在无线传感器网络实际应用中，通常根据应用需求来灵活地选择合适的网络拓扑结构。

5.2.1.2　拓扑发现

网络拓扑结构是一个重要的网络管理模型，它可以给出多个网络特征，如活动节点的数量、分布以及网络连通性。传统网络的拓扑结构一般是人工设置，整个网络的配置由网络管理员与用户共同完成。拓扑发现一般指网络管理员利用专用的网络管理软件自动生成网络的拓扑结构。与传统网络不同的是，无线传感器网络是一种自组织网络，网络的形成与运行在很大程度上是由多个网络节点自主完成的，并不需要人工配置。因此，在网络建立的初始阶段，需要采取一定的拓扑自主生成机制。

一般来说，簇是无线传感器网络拓扑结构的基本单位，无线传感器网络的拓扑结构通常由多个簇组成。类似于晶体生成方式，传感器网络可以有两种成簇方式：一种称为单晶方式，另一种称为多晶方式。在单晶方式中，网络中的簇都是由唯一的根节点发起形成，每一个申请加入簇的节点都要向根节点发出请求，根据根节点的不同响应，发出申请的节点可以加入已有簇或者形成新簇。在多晶方式中，所有节点均自发地发现其他节点并按某种规则形成独立的簇。随着各个簇的形成，簇之间可以建立起联系，当包含汇聚点的簇与其他的簇建立联系后，整个拓扑结构就生成了。图 5.23 是一个单晶方式生成的簇状树(cluster tree)结构，在 IEEE 802.15.4 标准中使用了此类结构[4]。

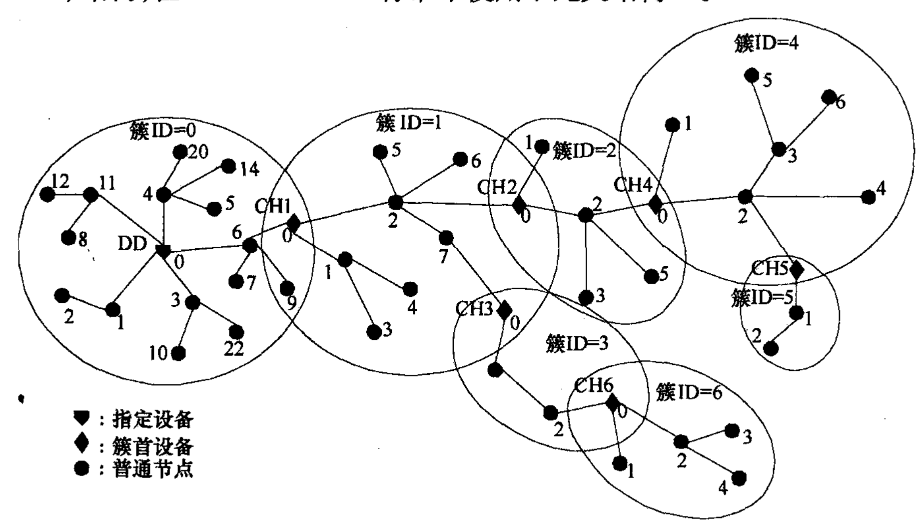


图 5.23　单晶方式生成的簇状树结构

单晶方式成簇使网络具有更好的可控性和安全性，但形成速度较慢；多晶方式则正相反，由于各个簇是在网络初始化阶段由节点自发形成的，网络可控性较差，安全性也不如单晶方式，但是整个网络的拓扑生成速度较快。

对于网络管理来说，两种方式所形成的簇都需要拓扑发现机制。如果采用单晶方式，尽管数据收集节点在网络初始就已了解整个网络的拓扑结构，但随着网络的运行，原有的拓扑结构必然发生变化。因此，数据收集节点需要采用拓扑发现机制来重新获取整个网络的当前拓扑结构；如果采用多晶方式生成簇，即使在网络形成的初始阶段，数据收集节点也要采用一定的拓扑发现机制来获取网络的拓扑信息。

拓扑发现面临着以下技术挑战：

(1)由于节点的实效及移动，无线传感器网络的拓扑结构需要具有自主调整能力，保

证整个网络的连通及某些 QoS 需求。

(2)由于能量限制,拓扑发现过程不能消耗过多的能量。

(3)小规模的网络可以采用平面结构,但对于大规模的无线传感器网络而言,分层的结构可能是比较实际的。

5.2.2　无线传感器网络拓扑控制

5.2.2.1　拓扑控制技术概述

传统的无线自组网络中,拓扑控制是指通过一定的机制自适应地将一定数目的节点组成一个互联网络。无线传感器网络作为一种新型的无线自组网络,同样需要拓扑控制的思想。与传统无线自组织网络相比,无线传感器网络具有自身的特点,如部署的环境更为复杂、多采用电池供电、能量更为有限、节点数目更多、节点部署更密集、网络拓扑变化更为频繁等,所以无线传感器网络需要一种更加优化和高效的拓扑控制机制[5]。

无线传感器网络拓扑控制主要研究的问题是,在保证网络的覆盖度和连通性的前提下设置或调整节点的发射功率,并按照一定原则选择合适的节点成为骨干节点参与网络中数据的处理和传输,达到优化网络拓扑结构的目的。具体来说,无线传感器网络中拓扑控制可以分为两个研究方向:功率控制和层次拓扑结构控制[6]。

功率控制机制调整网络中每个节点的发射功率,保证网络连通,均衡节点的直接邻居数目的同时,降低节点之间的通信干扰。层次拓扑控制是利用分簇思想,依据一定的原则使网络中的部分节点处于激活状态,成为簇头节点,由这些簇头节点构建一个连通的网络来处理和传输网络中的数据;其他节点则处于非激活状态,关闭其通信模块以降低能量消耗,并且定期或不定期地重新选择簇头节点以均衡网络中节点的能量消耗。

就无线传感器网络而言,高效优化的拓扑控制机制具有重要意义,具体表现在以下几个方面:

(1)降低节点能量消耗,延长网络生存时间。由于无线传感器网络中的节点多采用能量有限的电池供电,降低节点能量消耗是在整个网络的设计时需要主要考虑的目标之一。拓扑控制通过合理地调整节点的发射功率,并有选择性地让部分节点的通信模块关闭,使其处于非激活状态,以及定期或不定期更新簇头。均衡节点能量消耗的方法能在很大程度上降低节点的能量消耗,从而显著地延长整个网络的生存时间。

(2)为路由协议提供基础。路由协议需要获悉网络的拓扑结构,而且只有有效的节点才能够进行数据传输和转发;而无线传感器网络中的节点很容易因为能量耗尽或遭到破坏等原因而失效,以及新节点的加入都会引起网络拓扑的变化。拓扑控制机制正好可以调整节点之间的邻居关系,以及确定哪些节点处于活动状态,哪些节点处于非活动状态。

(3)有利于分布式算法的应用。无线传感器网络通常节点数目庞大,集中式的处理方法往往因为通信量太大和响应时间长而无法应用;而层次拓扑结构控制的分簇式管理思路有利于分布式算法的应用,适合大规模部署的网络。

(4)有利于数据融合。无线传感器网络中数据融合是指将多个传感器采集到的数据发送到某些节点,由这些节点按照一定的方法进行处理,以求得到较高质量(较高质量的确切涵义取决于具体应用)的信息。而这些参与多源数据处理的节点(即骨干节点)的选

择是拓扑控制的主要内容之一。

(5)降低节点通信干扰，提高网络吞吐量。无线传感器网络中节点通常部署密集，节点的发射功率合理选择是个微妙的问题。发射功率过大容易引起节点之间的干扰太强，增加误码率，降低无线通信效率和节点能量利用率；过小则难以保证网络的连通性。拓扑控制中的功率控制思想正是解决这个问题的重要方法。

5.2.2.2　拓扑控制研究现状及主要技术挑战

目前，国内外对拓扑控制的研究已经取得了一定的成果。在功率控制方面，已经提出的算法有 Kubisch 的 LMA(Local Mean Algorithm)/LMN(Local Mean Neighbors Algorithm)算法[7]、Ramanathan 的 LINT/LILT 算法[8]、Narayanaswamy 的 COMPOW 算法[9]、N. Li 的 DRNG(Directed Relative Neighborhood Graph)和 DLMST(Directed Local Minimum Spanning Tree)算法[10]。前三者主要是利用节点度数(直接邻居数目/单跳可达邻居数目)，第四种算法主要是以图论中的邻近图作为其理论基础。

在层次拓扑控制方面，已经提出的算法有 Deb 的 TopDisc(Topology Discovery)拓扑发现算法[11]、Santi 的改进 GAF(Geographical Adaptive Fidelity)分簇算法[12]、Heinzelman 的 LEACH(Low Energy Adaptive Clustering Hierarchy)算法[13]和 Younis 的 HEED 算法[14]等。这些算法为实现拓扑控制提供了一定的思路，不过也还存在有待改进的地方。例如，基于邻近图的算法所需信息过多且运算量也不小；TopDisc 算法没有考虑其鲁棒性的问题；改进的 GAF 算法的前提假设是节点能够获悉自己精确的位置信息，而节点位置信息的获取又是无线传感器网络中有待解决和正在研究的另一个重要问题——节点定位。

无线传感器网络中拓扑控制算法基本还处于理论研究或试验模拟阶段，应用于实际还存在一些困难，有待进一步研究。启发式的节点唤醒和休眠机制，在数据消息中携带网络拓扑控制信息的机制等也逐渐被引入拓扑控制的研究中。此外，传感器节点技术的发展使得节点具有更强的通信、计算、存储能力，这也为无线传感器网络的拓扑控制研究带来新的机会。

虽然无线传感器网络的拓扑控制研究已经取得一定的研究进展，但就其实用化来说还面临一些挑战：

(1)无线传感器网络通常属于大规模网络，拓扑控制算法需要有较快的收敛速度。

(2)节点的移动、失效或新节点的加入都会引起网络拓扑结构自身发生变化，这要求拓扑控制算法具有较强的自适应能力，能够保证网络的 QoS 需求。此外，在网络因为过多节点失效等原因而无法正常工作时，对追加节点数目和方位的预测可能也是拓扑控制的一项任务。

(3)节点能量非常有限，拓扑控制算法本身不能过于复杂，算法所引起的通信量也不能过多，要尽量降低拓扑控制算法的能量消耗。

5.2.3　无线传感器网络拓扑控制算法

5.2.3.1　功率控制算法

作为无线传感器网络中拓扑控制的研究方向之一，功率控制是指通过合理地设置或动态调整节点的发射功率，在保证整个网络连通的同时，降低节点之间的相互干扰，达到提高节点能量利用效率，延长网络生存时间的目的。

1. 基于节点度数的 LMA 和 LMN 算法

所谓节点的度数，是指与节点相距一跳的邻居节点的数目。基于节点度数的这一类功率控制算法的基本思想是限定节点度数的上限和下限，通过动态调整节点的发射功率使得节点度数处于上下限之间。这类算法在保证网络连通的同时，使得节点之间的链路具有一定的冗余性和可扩展性。下面介绍两种典型的基于节点度数的功率控制算法：LMA 算法和 LMN 算法。这两种算法都是周期性地调整节点的发射功率，其基本步骤相同唯一的区别在于计算节点度数的方法不同。LMA 算法和 LMN 算法都假定每个节点具有唯一的标识符 ID，LMA 的具体步骤如下：

(1)初始阶段所有节点具有相同的发射功率 P_{T0}，每个节点周期性地广播一个包含其 ID 的 LIFEMSG 消息。

(2) 当节点接收到 LIFEMSG 消息后，发送一个包含 LIFEMSG 的节点 ID 的应答消息 LIFEACKMSG。

(3)节点在下一次广播 LIFEMSG 之前，检查已经接收到的 LIFEACKMSG 应答消息数目，并以此数目作为其邻居节点数 N。

(4)如果 N 大于邻居节点数的上限 T_{max}，则该节点在本次广播 LIFEMSG 时将根据式(5.2)减小其发射功率，但不小于初始发射功率 P_{T0}的 B_{min}倍。类似地，如果 N 小于邻居节点数的下限 T_{min}，则该节点在本次广播 LIFEMSG 时将根据式(5.3)增大其发射功率，但最大不超过初始发射功率 P_{T0}的 B_{max}倍，即

$$P = \max\{B_{min}P_{T0}, A_{dec}(1 - (N - T_{max}))P_{T0}\} \tag{5.2}$$

$$P = \min\{B_{max}P_{T0}, A_{in}(T_{min} - N)P_{T0}\} \tag{5.3}$$

LMN 算法与 LMA 算法基本相同，唯一的区别在于计算邻居节点数的方法不同。在 LMN 算法中，每个节点回复的 LIFEACKMSG 应答消息包含有自己的邻居节点数。节点在收到所有邻居节点回复的 LIFEACKMSG 应答消息后，以这些应答消息中所包含的邻居节点数的平均值，即以邻居的邻居节点数的平均值作为自己的邻居节点数。

这两种方法对无线传感器节点的硬件要求不高，也不要求严格的时间同步。这两种算法只利用少量的局部信息；虽然都没有严格的理论推导，但试验仿真结果表明可以保证网络的收敛性和网络的连通性。

2. 基于邻近图的 DRNG 和 DLMST 算法

邻近图是相对另一个图而言的。所谓由图 $G=(V,E)$ 导出的邻近图 $G'=(V,E')$ 是指(其中，V 是图 G 中所有顶点的集合，E 是所有边的集合，E'为 E 的子集)对于任意一个顶点 $v \in V$，根据给定的邻近判断条件 q_t，E 中满足判断条件 q_t 的边$(u,v) \in E'$[15]。

基于邻近图的功率控制算法的主要思想：把所有节点处于最大发射功率状态下形成的网络拓扑图视为按照判断条件导出 G 的邻近图 G'，然后 G'中的每个节点根据与相距自己最远的邻居节点之间的距离来确定其发射功率。一般认为，无线传感器网络两节点之间的通信是对称的，即双向连通，因此在根据邻近图算法得到图 G'后还需要进行必要的边的增删，以确保最终的网络拓扑图是双向连通的。目前，无线传感器网络中基于邻近图理论的拓扑控制算法并不多，比较成熟的有 DRNG 和 DLMST 算法。

N. Li 的 DRNG(Directed R，lative Neighborhood Graph)和 DLMST(Directed Loral Mini-

mum Spanning Tree)[10]是从邻近图的角度实现拓扑控制的算法,以经典的邻近图(Relarive Neighborhood Graph,RNG)、局部最小生成树(Local Minimum Spanning Tree,LMST)为理论基础,着重提出了节点发射功率不一致时的拓扑控制解决思路。

为了便于叙述,预先作如下说明:

(1)节点 u 和 v 之间的连接是非对称的。对应地,顶点 u 和 v 之间的边 (u,v) 是有向的。

(2)R_u 表示节点 u 的无线电发射半径(Radio Range),$d(u,v)$ 表示节点 u 和 v 之间的距离,N_u^R 表示节点 u 以最大无线电发射半径时的可达节点集合(即可达邻居集)。可达邻居子图 G_u^R 是指由节点 u 和 N_u^R 以及这些节点之间的边构成的图。

(3)为每条边 (u,v) 赋予对应的权重函数 $\omega(u,v)$,且对于边 (u_1,v_1) 和 (u_2,v_2),其相应的权重函数 $\omega(u_1,v_1)$ 和 $\omega(u_2,v_2)$ 满足如下关系:

$$\omega(u_1,v_1) > \omega(u_2,v_2) \Leftrightarrow d(u_1,v_1) > d(u_2,v_2) \tag{5.4}$$

或

$$d(u_1,v_1) = d(u_2,v_2),\text{但}\max\{\mathrm{ID}(u_1),\mathrm{ID}(v_1)\} > \max\{\mathrm{ID}(u_2),\mathrm{ID}(v_2)\}$$

或

$$d(u_1,v_1) = d(u_2,v_2),\text{且}\max\{\mathrm{ID}(u_1),\mathrm{ID}(v_1)\} = \max\{\mathrm{ID}(u_2),\mathrm{ID}(v_2)\}$$

但

$$\min\{\mathrm{ID}(u_1),\mathrm{ID}(v_1)\} > \min\{\mathrm{ID}(u_2),\mathrm{ID}(v_2)\}$$

在 DRNG 和 DLMST 算法中,为了实现拓扑控制,节点需要获取有关邻居节点的一些信息,因此在算法初始阶段有一个邻居节点信息收集阶段。在此阶段中,每个节点以自己最大的发射功率广播 HELLO 消息(该消息包括节点 ID 和节点位置信息)。每个节点则根据接收到的 HELLO 消息确定自己的可达邻居集合 N_u^R。

DRNG 算法中,其邻居节点的判断标准如图 5.24 所示。如果节点 u 和 v 的距离满足条件 $d(u,v) < R_u$,并且不存在节点 i 同时满足条件 $\omega(u,i) < \omega(u,v)$,$\omega(i,v) < \omega(u,v)$,$d(i,v) \leq R_i$,则节点 v 为节点 u 的邻居节点。

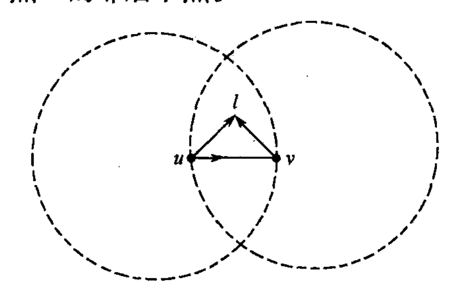


图 5.24　DRNG 算法中的邻居节点判断标准

从本质上说,DLMST 算法等价于求解可达邻居子图 G_u^R 的最小生成树。具体方法如下:

(1)节点 u 确定其可达邻居子图 G_u^R。

(2)将 u 与所有可达邻居节点的边所对应的权重函数 $\omega(u,v)$ 按照升序排序。

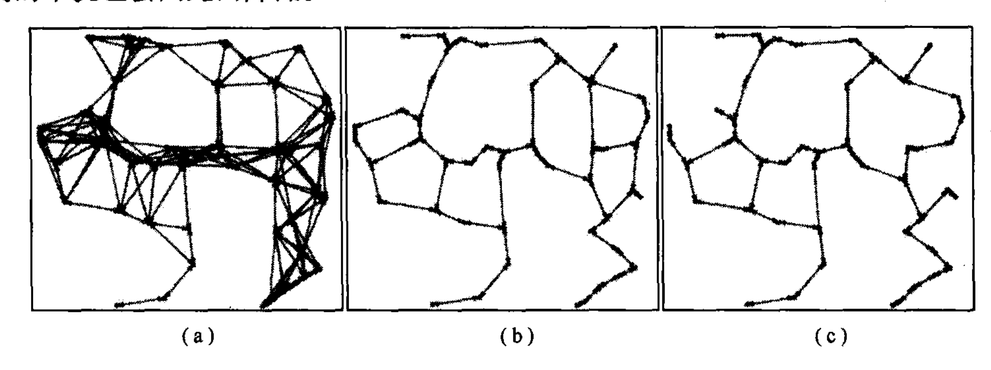
(3)从小到大依次取出这些权重函数对应的边(认为这些边属于 G_u^R 的邻近图),直到

u 与 G_u^R 中的每个节点都直接或间接连通。

(4)与 u 直接连通的邻居节点构成 u 的邻居节点集。

在节点 u 确定其邻居节点集之后，将根据相距最远的邻居节点之间的距离来调整自己的发射功率，即使得相距最远的邻居节点恰好处于节点 u 的无线电发射半径之内。此外，正如前面提到的，为了保证网络的双向连通性，还需要对 G_u^R 的邻近图进行必要的边的增删。

图5.25是DRNG和DLMST算法对网络拓扑优化的示例。从图中可以看出，通过DRNG或DLMST算法的优化，网络拓扑明显简化。这归因于节点发射功率的调整，节点之间的干扰也会因此而降低。



(a) (b) (c)

图5.25 DRNG和DLMSP算法对网络拓扑优化的示例

(a)原始网络拓扑图；(b)DRNG优化后的拓扑图；(c)DLMST优化后的拓扑图。

DRNG和DLMST充分利用邻近图理论，结合传感器网络的特点，针对节点发射功率不一致的问题提出了一种解决方法；同时考虑到网络的连通性，并通过必要的增删操作来保证优化后的拓扑保持双向连通。

5.2.3.2 层次拓扑结构控制算法

无线传感器网络中，节点的无线通信模块处于发送状态下的功耗最高，接收状态和空闲状态次之，休眠状态功耗最低。例如，目前用于无线传感器网络的主流传感器Berkeley Motes的通信模块处于发送状态的功耗为60mW，接收状态和空闲状态的功耗均为12mW，休眠状态下的功耗仅为0.03mW，四者的功耗对比达到2000:400:400:1，因此，降低能耗的关键是降低网络内的通信流量，使更多的节点在更长时间段处于休眠状态。为了大幅度降低无线通信模块的能量消耗，可以考虑依据一定的机制选择部分节点作为骨干节点，这些节点的通信模块处于打开状态；而关闭其他非骨干节点的通信模块。由骨干节点构建一个连通的网络来处理和传输数据。在这种机制下，节点被分为骨干节点和非骨干节点两类，骨干节点对非骨干节点进行管辖。这类算法将网络分为相连的区域，一般称为分簇算法。

1. TopDisc算法

TopDisc(Topology Discovery)[11]算法是基于最小支配集理论的经典算法。它首先由初始节点发出拓扑发现请求，通过广播该请求消息来确定网络中的骨干节点，并结合这些骨干节点的邻居节点的信息形成网络拓扑的近似拓扑。在这个近似拓扑形成以后，为了减小算法本身引起的网络通信量，只有骨干节点才对初始节点拓扑发现请求做出相应的

响应。

为了确定网络中的骨干节点，TopDisc 算法采用的是贪婪算法[16]。具体地，TopDisc 提出了两种类似的方法：三色法和四色法。

在三色法中，节点可以处于3种不同状态。在 TopDisc 算法中，分别用白色、黑色、灰色3种颜色表示：

(1)白色为尚未被发现的节点，或者说是没有接收到任何拓扑发现请求的节点。

(2)黑色为骨干节点(簇头节点)，负责响应拓扑发现请求。

(3)灰色为普通节点，至少被一个标记为黑色的节点覆盖，即黑色节点的邻居节点。

在初始阶段，所有节点都被标记为白色，算法由一个初始节点发起，算法结束后所有节点都将被标记为黑色或者灰色(前提假设整个网络拓扑是连通的)。TopDisc 采用两种启发式方法来使得每个新的黑色节点都尽可能多地覆盖还没有被覆盖的节点：一种是节点颜色标记方法；另一种是节点转发拓扑发现请求时将会故意延时一段时间，延时时间的长度反比于该节点与发送拓扑发现请求到该节点的节点之间的距离。

三色法的详细过程描述如下：

(1)初始节点被标记为黑色，并向网络广播拓扑发现请求。

(2)当白色节点收到来自黑色节点的拓扑发现请求时将被标记为灰色，并在延时时间 T_{WB}后继续广播拓扑发现请求。T_{WB}反比于它与黑色节点之间的距离。

(3)当白色节点收到来自灰色节点的拓扑发现请求时，将在等待时间 T_{WG}后标记为黑色，但如果在等待期间又收到来自黑色节点的拓扑发现请求则优先标记为灰色；同样，等待时间 T_{WG}反比于该白色节点与灰色节点之间的距离。不管节点被标记为灰色还是黑色，都将在完成颜色标记后继续广播拓扑发现请求。

(4)所有已经被标记为黑色或者灰色的节点，都将忽略其他节点的拓扑发现请求。

为了使得每个新的黑色节点都尽可能多地覆盖还没有被覆盖的节点，TopDisc 采用了反比于节点之间距离的转发延时机制。其合理性简单解释如下：理想情况下，节点的覆盖范围是半径为无线电发射半径的圆。于是，单个的节点所能够覆盖的节点数目正比于其覆盖面积和局部的节点部署密度。对于一个正在转发拓扑发现请求的节点，它所能够覆盖的新的节点(还没有被任何节点覆盖的)则正比于它的覆盖面积与已经覆盖的面积之差。

【例5.1】如图5.26所示，假设节点 a 是初始节点，根据步骤(1)它被标记为黑色，并广播拓扑发现请求。节点 b 和节点 c 收到来自节点 a 的拓扑发现请求，根据步骤(2)被标记为灰色，并各自等待一段时间后广播拓扑发现请求。假设节点 b 比节点 c 距离节点 a 更远，即节点 b 的等待时间更短，于是节点 b 先广播拓扑发现请求。节点 d 和节点 e 收到来自节点 b 的拓扑发现请求，根据步骤节点(3)各自等待一段时间，节点 a 已经被标记为黑色，根据步骤(4)它会忽略节点 b 的拓扑发现请求。假设节点 d 比节点 e 距离节点 b 更远，则节点 d 比节点 e 更有可能标记为黑色，此处假设节点 d 和节点 e 都因为等待期间内没有收到来自黑色节点的拓扑发现请求而标记为黑色。注意，在标记为黑色的两个节点之间存在一个中

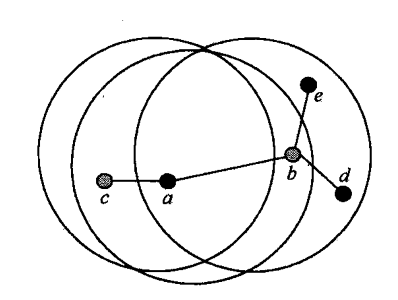


图5.26　三色法示意图

介节点(图中为节点 b)同时被这两个黑色节点覆盖,这归因于三色法的内在性质。

可以看出,三色法所形成的簇之间存在重叠区域。为了增大簇之间的间隔,减少重叠区域,TopDisc 算法同时也提出了四色法。顾名思义,节点可以处于 4 种不同的状态,分别用白色、黑色、灰色和深灰色表示。前 3 种颜色代表的含义跟三色法相同,增加的深灰色表示节点收到过拓扑发现请求,但不被任何标记为黑色的节点覆盖。

与三色法类似,在初始阶段,所有节点都被标记为白色,算法由一个初始节点发起,算法结束后所有节点都将被标记为黑色或者灰色(前提假设整个网络拓扑是连通的,注意最终没有标记为深灰色的节点)。

四色法的详细过程描述如下:

(1)初始节点被标记为黑色,并向网络广播拓扑发现请求。

(2)当白色节点收到来自黑色节点的拓扑发现请求时,将标记为灰色,并在延时时间 T_{WB}后继续广播拓扑发现请求。T_{WB}反比于它与黑色节点之间的距离。

(3)当白色节点收到来自灰色节点的拓扑发现请求时,将标记为深灰色并继续广播拓扑发现请求,然后等待一段时间(同样与距离成反比)。如果在等待期间收到来自黑色节点的拓扑发现请求,则改变为灰色,否则它自己成为黑色。

(4)当白色节点收到来自深灰色节点的拓扑发现请求时,等待一段时间(同样与距离成反比)。如果在等待期间收到来自黑色节点的拓扑发现请求,则改变为灰色,否则它自己成为黑色。

(5)所有已经被标记为黑色或者灰色的节点都将忽略其他节点的拓扑发现请求。

【例 5.2】如图 5.27 所示,假设节点 a 是初始节点,根据步骤(1)它被标记为黑色,并广播拓扑发现请求。节点 b 收到来自节点 a 的拓扑发现请求,根据步骤(2)被标记为灰色,并各自等待一段时间后广播拓扑发现请求。节点 c 和节点 e 都接收到来自节点 b 的拓扑发现请求,根据步骤(3),被标记为深灰色,继续广播拓扑发现请求启动计时器(即等待一段时间)。节点 d 收到来自节点 c 的拓扑发现请求,根据步骤(4)等待一段时间,假设这段时间内没有收到任何来自标记为黑色节点的拓扑发现请求,于是节点 d 标记为黑色,并广播拓扑发现请求。假设节点 c 在等待期间收到了节点 d 的拓扑发现请求,被标记为灰色。假设节点 e 在等待期间没有收到任何来自标记为黑色节点的拓扑发现请求,被标记为黑色。

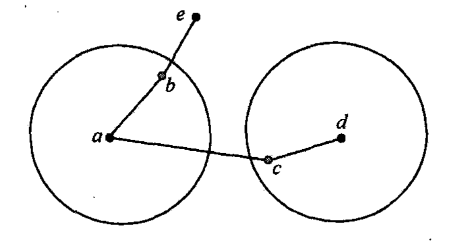


图 5.27　四色法示意图

与三色法相比,四色法形成的簇数目更少,簇与簇之间的重叠区域也更小。但是可能形成一些孤立的标记为黑色的节点(如图 5.27 中的节点 e)不覆盖任何灰色节点。虽然三色法和四色法所形成的黑色节点数目相当,但四色法中传输的数据量要少一些。

TopDisc 算法利用图论中的典型算法,提出了一种有效方法来构建网络的近似拓扑,是分簇算法中的经典算法。它是一种只需要利用局部信息、完全分布式的、可扩展的网络拓扑控制算法。不过也存在有待改进的地方,如算法开销偏大,另外没有考虑节点的剩余能量。

2. GAF 算法及其改进算法

GAF(Geographical Adaptive Fidelity)[17]算法是针对无线传感器网络节点部署密集的

特点提出来的。它根据节点的地理位置信息和节点的无线电发射半径将网络部署区域划分为虚拟单元格。节点按照其位置信息被划入到相应的单元格中。从分组转发的角度来看,地理位置邻近的节点在数据转发过程中所起的作用基本是等价的,所以 GAF 算法使每个虚拟单元格中保待只有一个节点处于活动状态(即为簇头节点),其他节点处于非活动状态。

GAF 算法中,每个节点可以处于 3 种不同状态:休眠、发现和活动状态。状态间的转换过程如图 5.28 所示。

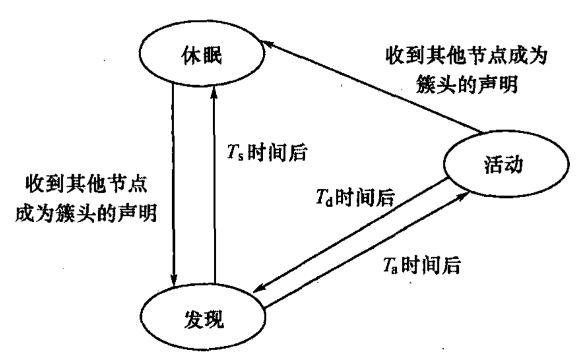


图 5.28　GAF 算法中节点状态转换图

初始状态下,所有节点处于发现状态。当节点处于发现状态下,节点交换 Discovery 消息来获得同一虚拟单元格中其他节点的信息。Discovery 消息由节点 ID、节点状态、虚拟单元格 ID、节点活动时间估计等信息组成。节点根据其位置信息和虚拟单元格大小确定虚拟单元格的 ID。

当节点进入发现状态时,它设置一个计时器 D_t。一旦计时器 D_t 超过 T_d,节点广播 Discovery 消息,同时转换到活动状态。如果在计时器超时之前,节点收到其他节点成为簇头节点的声明,则取消计时器,关闭无线电发射模块,进入休眠状态。计时器的设置降低了多个节点同时成为簇头节点,发生冲突的概率。

当节点进入活动状态时,它设置一个计时器 A_t,表示节点将处于活动状态的时间。一旦计时器 A_t 超过 T_d,节点转换到发现状态。在节点处于活动状态期间。以时间间隔 T_d 重复广播 Discovery 消息,以便压制其他处于发现状态的节点进入活动状态。在计时器 A_t 超时 T_a 后,节点转入发现状态。当节点进入休眠状态时,启动一个计时器 A_t,在 A_t 超时之后转入到发现状态。

GAF 算法采用负载均衡策略使得节点的能量消耗尽量均衡,以延长网络生存时间。其背后的思想是把网络中的所有节点视为等同地位,没有理由过于“处罚”其中某些节点。GAF 算法采用负载均衡策略具体描述如下:节点在保持活动状态 T_a 时间后,转换到发现状态,使得同一虚拟单元格中的其他节点有机会进入活动状态成为簇头节点。节点剩余能量越多,成为簇头节点的几率就越大。由于旧的簇头节点处于活动状态时,虚拟单元格中的其他节点都处于休眠状态,由此旧的簇头节点的剩余能量很可能就少很多,于是它继续本轮簇头竞争中成为簇头节点的几率就小一些。仿真实验表明,GAF 算法所延长的网络生存周期正比于节点密度,即虚拟单元格中的平均节点数。

GAF 算法是无线传感器网络研究领域中较早采用让部分节点进入休眠状态以减小

能量消耗的拓扑控制算法。GAF算法提出的节点状态转换机制和按虚拟单元格划分簇的思想具有重要意义。不过它是基于平面模型，并没有考虑到实际网络中节点之间距离的邻近并不能代替节点之间的直接通信问题。另外很重要一点是，它的前提是假设节点能够获悉自己精确的位置信息，而节点位置信息的获取又是无线传感器网络中有待解决和正在研究的另一个重要问题——节点定位。

Stani提出了一种改进型的GAF算法[12]。在改进的算法中设计了两种不同的簇头选择机制GAF-FULL簇头选择法和GAF-RANDOM簇头选择法。

在GAF-FULL簇头选择法中，需要每个节点能够预先获得其自身的位置、虚拟单元格ID，同一虚拟单元格中其他节点的ID，全局的网络时间（用于时间同步）等信息。具体的簇头选择方法如下：对于某个虚拟单元格，假设其中有N个节点，分别编号为0，1，…，$N-1$。初始时刻为T_0，下述每步操作需要时间T_s。对于节点$n\neq 0, N-1$：

(1)在$T_0+(n-1)\times T_s$时刻，打开通信模块，接收来自节点$n-1$的消息$M=(E_{max}, m)$，此处E_{max}和m分别表示本虚拟单元格的所有节点中最大剩余能量和对应的节点ID。假设节点n估计当本次算法执行完毕后剩余能量为E_p，则按照$E_{max}=\max\{E_{max}, E_p\}$以及如果$E_{max}=E_p$，则$m=p$的规则修改消息$M=(E_{max}, m)$。

(2)在$T_0+n\times T_s$时刻，发送消息$M=(E_{max}, m)$然后关闭通信模块。

(3)在$T_0+N\times T_s$时刻，打开通信模块，接收消息$M=(E_{max}, m)$，此时m是新产生的簇头ID，E_{max}是其剩余能量。如果$n\neq m$，则关闭通信模块。

对于节点0和节点$N-1$，其执行过程有些不同：节点0在T_0时刻发送消息$(E_0, 0)$，然后在$T_0+N\times T_s$执行上述的步骤(3)；节点$N-1$在$T_0+N\times T_s$时刻发送消息$M=(E_{max}, m)$，如果发现自己不是簇头节点，则关闭通信模块。对于一个含有4个节点的虚拟单元格，整个执行过程如图5.29所示。

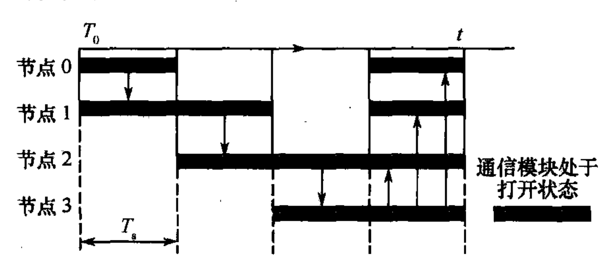


图5.29 GAF-FULL簇头选择法的时序($N=4$)

在实际情况中，节点很可能无法获得所在虚拟单元格中所有节点的信息，这时GAF-FULL簇头选择法就不再适用。对此，Stani提出了另外一种方法GAF-RANDOM簇头选择法。该方法假设每个节点具有预先获得其自身的位置、所在虚拟单元格ID，全局的网络时间（用于时间同步）以及检测无线信道冲突等能力。对于虚拟单元格中的某个节点n，其GAF-RANDOM簇头选择法执行过程的伪码[12]描述如表5.1所列。

上述伪码的详细解释如下：节点n随机判决它是否成为簇头节点（判决成为簇头节点的概率为p）。如果判决成为簇头节点，则发送消息$M_m=(E_n, n)$；如果判决不成为簇头节点，则节点进入侦听接收状态，等待其他成为簇头节点广播消息M_m。如果在本次簇头竞争中没有任何节点判决自己成为簇头节点，或者由多个节点判决成为簇头节点，则重新

表 5.1　簇头选择法伪码

```
END = false;
While(END = = false)
{
    以成功概率为 p 进行随机判决;
    如果判决成功,发送消息 M_m = (En,n);否则节点进入侦听接收状态;
    如果没有收到其他任何节点发送的消息 M 或者其他节点消息发生冲突,则继续;
    END = true;
    如果本次判决失败,则关闭通信模块
}
```

开始新一轮的簇头选择。如果节点 n 没有成功成为簇头节点,并且有其他节点成功成为簇头节点,则节点 n 关闭其通信模块。

令 S_c 表示上述循环测试直到产生新的簇头节点为止所循环的次数。显然,S_c 依赖于判决成功概率 p,并且 S_c 服从参数为 $(1-q)$ 的几何分布 $q=1-Np(1-P)^{N-1}$,那么到产生新的簇头节点为止循环次数小于 k 的概率 $P_r(S<k)=1-q^k$ 随着 k 的增大收敛于 1,且 q 值越小收敛速度越快。理所当然,q 值越小算法性能越好。很简单,q 在 $p=1/N$ 时取得最小值 $1-(1-1/N)^{N-1}$,当 N 非常大时,$q \approx l-1/\mathrm{e}$。因此,合理设置成功判决概率,可使得产生新的簇头节点之前循环测试的次数 S_c 的期望值 $E(S_c)=1/(1-q)\approx e$,这在实际网络分簇算法中是可以接受的。

Stani 提出了这两种簇头选择方法依然是针对节点部署密度高的情况,算法所延长的网络生存周期正比于节点密度。有待进一步讨论的是,这两种方法仍旧需要节点具有获悉自己精确的位置信息能力,这对无线传感器网络本身也是需要解决的关键技术。此外,它们还假设同一虚拟单元格中节点之间保持时间同步,而时间同步也是无线传感器网络中正在研究的热点问题。

5.2.3.3　启发式拓扑控制算法

传感器网络通常是面向应用事件驱动的网络,骨干网节点在没有检测到事件时不必一直保持在活动状态。在传感器网络的拓扑控制算法中,除了传统的功率控制和层次型拓扑控制两个方面之外,也提出了启发式的节点唤醒和休眠机制。该机制能够使节点在没有事件发生时设置通信模块为睡眠状态,而在有事件发生时及时自动醒来并唤醒邻居节点,形成数据转发的拓扑结构。这种机制的引入使得无线通信模块大部分时间都处于关闭状态,只有传感器模块处于工作状态。由于无线通信模块消耗的能量远大于传感器模块,所以这进一步节省了能量开销。这种机制重点在于解决节点在睡眠状态和活动状态之间的转换问题,不能够独立作为一种拓扑结构控制机制,需要与其他拓扑控制算法结合使用。

1. STEM 算法

STEM(Sparse Topology and Energy Management)算法[18]是较早提出的节点唤醒算法。在 STEM 算法中,节点需要采用一种简单而迅速的节点唤醒方式,保证网络通信的畅通和较小的时延。STEM 算法包含两种不同的机制 STEM-B 和 STEM-T。

1)STEM-B(STEM-BEACON)算法

当一个节点想给另外一个节点发送数据时,它作为主动节点先发送一串 beacon 数据

包。目标节点在收到 beacon 数据包后，发送应答信号并自动进入数据接收状态。主动节点接收到应答信号后，进入数据发送阶段。为了避免唤醒信号和数据通信的冲突，STEM－B算法使用侦听信道与数据传输信道两个分离信道。

图 5.30 所示为 STEM-B 算法示意图，表示了节点 A 在一段时间内通信的能量消耗过程。节点 A 使用 f_1 和 f_2 两个信道，f_1 信道为侦听信道，f_2 信道为数据传输信道。节点 A 在侦听信道保持周期性的短时间侦听，在 $t_1 \sim t_5$ 时间内，节点 A 分别与节点 B 和节点 C 通信。在 t_1 时刻，节点 A 需要和邻居节点 B 进行通信，首先在频率为 f_1 的信道上发送一串 beacon 数据包，直到 t_2 时刻收到来自节点 B 的响应为止：节点 A 在 $t_2 \sim t_3$ 时段内通过 f_2 信道发送数据给节点 B，通信完成后暂时关闭 f_2 信道。在 t_4 时刻，节点 A 在 f_1 信道上侦听到节点 C 发送的 beacon 数据包，于是在 $t_4 \sim t_5$ 时段内通过 f_2 信道接收节点 C 发送的数据；在 t_5 之后，节点 A 关闭 f_2 信道，并继续保持在 f_1 信道上的侦听。可见，如果没有数据通信，节点 A 大部分时间只保持在 f_1 信道上的周期性侦听，很大程度上节省了能量消耗。

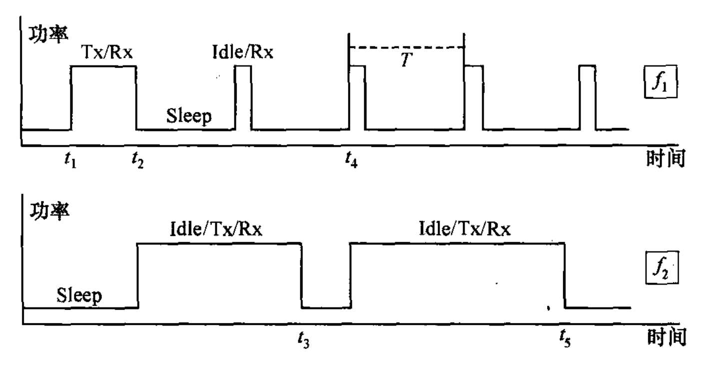


图 5.30　STEM-B 算法示意图

2）STEM－T（STEM－TONE）算法

STEM－T 算法比 STEM－B 算法简单，其节点周期性地进入侦听阶段，探测是否有邻居节点要发送数据。当一个节点想与某个邻居节点进行通信时，首先发送一连串的唤醒包，发送唤醒包的时间长度必须大于侦听的时间间隔，以确保邻居节点能够收到唤醒包。然后节点直接发送数据包。所有邻居节点都能够接收到唤醒包并进入接收状态。如果在一定时间内没有收到发送给自己的数据包，就自动进入睡眠状态。可见 STEM－T 算法与 STEM－B 算法相比省略了请求应答过程，但增加了节点唤醒次数。

STEM 算法使节点在整个生命周期中多数时间内处于睡眠状态，适用于类似环境监测或者突发事件监测等应用，这类应用均由事件触发，不要求节点时刻保持在活动状态。目前 STEM 算法可以与很多分簇类型的拓扑算法结合使用，如 GAF 算法等。值得注意的是，在 STEM 算法中，节点的睡眠周期、部署密度以及网络的传输延迟之间有着密切的关系，要针对具体的应用要求进行调整[18]。

2. ASCENT 算法

ASCENT（Adaptive Self-Configuring sensor Networks Topologies）算法[19]虽然与 STEM 算法同属于节点唤醒机制，但它们之间存在较大差别。ASCENT 算法着重于均衡网络中骨干节点的数量并保证数据通路的畅通。节点接收数据时若发现丢包严重就向数据源方向的邻居节点发出求助消息；节点探测到周围的通信节点丢包率很高或者收到邻居节点

发出的帮助请求时，它醒来后主动成为活动节点，帮助邻居节点转发数据包。

运行ASCENT算法的网络包括触发、建立和稳定3个主要阶段。触发阶段如图5.31(a)所示，当汇聚节点与数据源节点不能正常通信时，汇聚节点向它的邻居节点发出求助信息；建立阶段如图5.31(b)所示，是指当节点收到邻居节点的求助消息时，通过一定的算法决定自己是否成为活动节点，如果成为活动节点，就向邻居节点发送通告消息，同时这个消息是邻居节点判断自身是否成为活动节点的因素之一；稳定阶段如图5.31(c)所示，当数据源节点和汇聚节点间的通信恢复正常时，网络中活动节点个数保持稳定，从而达到稳定状态。稳定阶段保持一定时间后，由于个别节点能量耗尽或者外界干扰等因素，网络中又会出现通信不畅的现象，节点再次进入触发阶段。

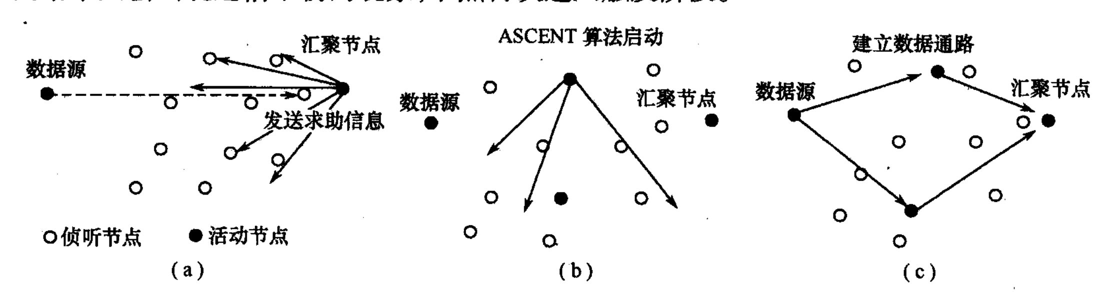


图5.31　ASCENT算法的3个阶段

(a)触发阶段；(b)建立阶段；(c)稳定阶段。

在ASCENT算法中，节点可以处于4种状态：休眠状态，即节点关闭通信模块，能量消耗最小；侦听状态，即节点只对信息进行侦听，不进行数据包的转发；测试状态，这是一个暂态，参与数据包的转发，并且进行一定的运算，判断自己是否需要变为活动状态；活动状态，节点负责数据包的转发，能量消耗最大。这4种状态之间的转换关系如图5.32所示，其中，NT表示节点的邻居数上限，LT表示丢包上限，T_s表示睡眠状态定时器，T_p表示侦听态定时器，T_t表示测试态定时器，neighbors代表邻居数，loss代表丢包率，help代表求助消息。

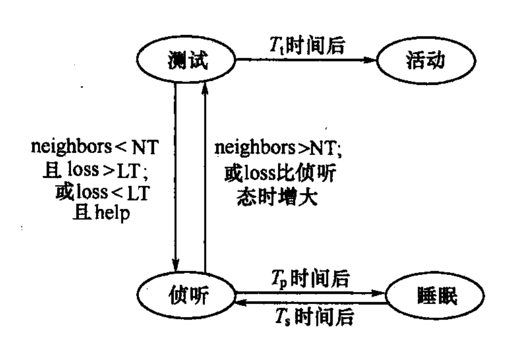


图5.32　ASCENT算法状态转换图

图5.32中状态之间的转换关系如下：

(1)休眠态与侦听态。处于休眠态的节点设置定时器T_s，当定时器超时后，节点由休眠态进入侦听态；处于侦听态的节点设置定时器T_p，当定时器超时后，节点由侦听态进入休眠态。

(2)侦听态与测试态。处于侦听态的节点侦听信道,如果发现当邻居数小于邻居上限,且信道的平均丢包率大于丢包上限,节点进入测试态;或者当平均丢包率小于丢包上限,但接收到来自邻居节点的求助消息时,节点也进入测试态。处于测试态的节点在定时器 T_t 超时前发现邻居数超过邻居数上限,或者平均丢包率比该节点进入测试态前还大时,说明该节点不适合成为活动节点,它将进入测试态。

(3)测试态与活动态。处于测试态的节点如果在定时器 T_t 超时前一直没有满足跳转到侦听态的条件,则在定时器超时后进入活动态,负责数据转发。

通过 ASCENT 算法,节点能够根据网络情况动态地改变自身状态,从而动态地改变网络拓扑结构,并且节点只根据本地信息进行计算,不依赖于无线通信模型、节点的地理分布和路由协议。但 ASCENT 算法有待完善的地方还很多,例如,应该针对更大规模的节点分布进行改进,并加入负载平衡技术等。

目前,传感器网络拓扑控制的研究有了初步的进展,提出了很多的拓扑控制算法,但是大多数算法都停留在理论研究阶段或者只做过少量节点的模拟,没有充分考虑实际应用的诸多困难。例如,节点大规模撒布时,如何保证算法的收敛速度,如何减小外界因素对通信的干扰,以及节点失效后如何追加等。此外,随着传感器节点技术的发展,节点有能力获得诸如精确的地理位置、周边环境情况等更多信息,并具有更强的计算能力,可以进一步提高网络拓扑控制的执行效率和精度。

现在的拓扑控制研究的发展趋势是以实际应用为背景,多种机制结合使用,强调网络拓扑控制的自适应性和鲁棒性[20],在保证网络连通性和覆盖性的前提下,提高网络通信效率,最大限度地节省能量来延长整个网络的生存时间。

参考文献

[1] Dunkel A, Alonso J, Voigt T. Marking TCP/IP Viable for Wireless Sensor Networks. In Proceedings of the Work-in-progress session of the 1st European workshop on wireless sensor networks, Technical report TKN-04-001 of Technical University Berlin, Telecommunication networks Group, Berlin, Germany, January 2004.

[2] Wei Ye, John Heidemann, Deborah Estain. An Energy Efficient MAC Protocol for Wireless Sensor Network [A]. In proceeding of INFOCOM 2002. San Francisco[C]: IEEE Computer Society 2002.

[3] Alec Woo, David E Culler. A Transmission Control Scheme for Media Access in Sensor Networks[A]. In proceeding of the ACM MobilCom2001 Rome[C]: ACM Press, 2001.

[4] Callaway E H. Wireless Sensor Networks: Architectures and Protocols[M]. Auerbach Publications, 2004

[5] Akyildiz I F, Su W, Sankatasubramaniam Y, et al. A Survey on Sensor Networks[J]. IEEE Communications Magazine, 2002, 40(8): 102 - 114

[6] Bao L, Garcia-Luna-Aceves J J. Topology Management in Ad Hoc Networks[C]. In Proceeding of the 4th ACM International Symposium on Mobile, 2006.

[7] Kubisch M, Karl H, Wolise A, etc. Distributed Algorithms for Transmission Power Control in Wireless Sensor Networks [C]. In Proceeding of IEEE Wireless Communications and Networking Conference (WCNC 2003), March 2003: 558 - 563.

[8] Ramanathan R, Rosales-Hain R. Topology Control of Multihop Wireless Networks Using Transmit Power Adjustment[C]. In Proceeding of IEEE Conference on Computer Communications(INFOCOM), March 2000: 404 - 413.

[9] Narayanaswamy S, Kawadia V, Sreenivas R S, etc. Power Control in Ad-Hoc Networks: Theory, Architecture, Algorithm and

Implementation of the COMPOW Protocol[C]. In Proceeding of European Wireless Conference, Feb, 2002: 156 - 162.

[10] Li N, Hou J C. Topology Control in Heterogeneous Wireless Networks: Problems and Solutions[C]. In Proceeding of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004), March 2004: 232 - 243.

[11] Deb B, Bhatangar S, Nath B. A Topology Discovery Algorithm for Sensor Networks with Applications to Network Management[R]. DCS Technical Report DCS-TR-441, Rutgers University, 2001.

[12] Santi P, Simon J. Silence is Golden with High Probability: Maintaining a Connected Backbone in Wireless Sensor Networks[C]. In Proceeding of 1st European Workshop on Woreless Sensor Networks (EWSN 2004), Jan 2004: 106 - 121.

[13] Heinzelman W, Chandrakasan A, Balakrishnan H. An Application-Specific Protocol Architecture for Wireless Microsensor Networks[J]. IEEE Transactions on Wireless Communications, October 2002, 1(4): 660 - 670.

[14] Younis O, Fahmy S. Distributed Clustering in Ad-Hoc Sensor Networks: A Hybrid, Energy-Efficient Approach[C]. In Proceeding of the IEEE Conference on Computer Communications (INFOCOM), Mar, 2004: 629 - 640.

[15] Toussaint G. The Relative Neighborhood Graph of Finite Planar Set[J]. Pattern Recognition, 1980, 12(4): 261 - 268.

[16] Thomas H C, Charles E L, Ronald L R. Introduction to Algorithms[M]. Second Edition. The MIT Press, 2002

[17] Xu Y, Heidemann J, Estrin D. Geography-Informed Energy Conservation for Ad Hoc Routing[C]. In Proceeding of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), July 2001: 70 - 84.

[18] Schurgers C, Tsiatsis V, Ganeriwal S, etc. Topology management for sensor netwroks: Exploiting latency and density. In: Proc 3rd ACM Int'l Symp on Mobile Ad Hoc Networking & Computing, Lausanne, Switzerland. June 9 - 11, 2002: 135 - 145.

[19] Cerpa A, Estrin D. ASCENT: Adaptive self-configuring sensor networks topologies. In: Proc 11th Joint Conf on IEEE Computer and Communications Societies (INFOCOM), New York, NY, June 2002.

[20] Wang X, Xing G, Zhang Y, etc. Integrated coverage and connectivity configuration in wireless sensor networks. In: Proc ist Int'l Conf on Embedded Netwroked Sensor Systems (SenSys'03), Los Angeles, CA. November 2003.

第6章　无线传感器网络覆盖与连通

无线传感器节点根据一定协议和网络拓扑结构生成无线传感器网络,并通过相互协作完成复杂的测量任务。当无线传感器节点无法实现确定布置时,如军事现场、人不可接触的危险地域、突发事件的应急处理等情景,采用随机布置方法实用性最强;当无线传感器节点能精确按照预先设定的方案进行人工或机械布置时,则可以事先确定相应的布置方法,以简化网络生成步骤和周期,提高无线传感器网络的覆盖效率。

无线传感器网络覆盖与连通问题是无线传感器网络研究的基本问题与重要问题之一。无线传感器网络的覆盖面积是用于衡量无线传感器网络测量性能的重要指标,该指标与无线传感器节点的类型及应用目标有关。为了保证无线传感器网络的测量有效性,通常要求监测范围内的任意一点都至少处于一个无线传感器节点的测量范围内。

无线传感器网络覆盖问题的基础是网络系统的能量有效性。一般而言,对于某项测量任务,传感器节点的布置数量都超过其需要量。这样,一方面可以弥补传感器节点定位精度不高所导致的测量精度降低的问题,另一方面也可以进一步提高系统容错性。但以能量有效性为核心的无线传感器节点硬件设计和网络协议将受到严格约束,如何在最小化传感器节点数量的前提下扩大无线传感器网络覆盖范围是一项值得研究的问题。

无线传感器网络覆盖问题与网络节点连通性密切相关,研究连通性的主要目的就是通过不同拓扑连接控制方法实现有效链路连接、减少干扰、保存和节省能量、有效地增加网络覆盖,从而最终改善网络性能。连通性决定了网络拓扑结构的可靠性,它的好坏直接决定了网络可靠性保障和拓扑连通性能。

6.1　无线传感器网络覆盖与连通问题概述

在介绍无线传感器网络覆盖与连通问题前,先简要看看网络部署问题。网络部署是无线传感器网络研究领域的基本问题之一,是确保无线传感器网络高效执行任务的第一步。由于每个网络节点的感知范围有限,多个网络节点的协作才可能感知整个监测区域,而部署则直接决定了传感器网络的感知范围能否覆盖整个监测区域。无线传感器网络部署就是根据允许的部署方式和应用需求,实现将适量的节点布置在监测区域内的适当位置。

网络部署必须满足两个方面的要求:一是感知范围必须覆盖整个监测区域;二是部署必须满足应用提出的在代价、能耗和可靠性等方面的需求。

传感器网络部署的具体研究内容取决于采用的部署方式,不同的应用环境决定了应

该采用何种部署方式。传感器网络常用的部署方式有确定放置和随机抛撒两种：确定放置，即通过操纵机器人或者人工安装等方式将节点放置在预定的确定位置上，这种方式适用于在安全监测区域内部署传感器网络，且节点没有移动能力的应用环境；随机抛撒，即通过炮弹弹射或飞机抛撒等方式将节点随机地散布在监测区域内，这种方式适用于在人不可接触的危险监测区域内部署传感器网络。

根据采用的部署方式，无线传感器网络部署的研究内容主要有以下几个方面：

(1)若采用确定放置的方式，需要设计算法来计算节点在监测区域内的预定位置。传感器网络的开发人员可以提前运行这种算法，根据计算结果来部署无线传感器网络。

(2)若采用随机抛撒的方式，需要设计算法计算节点在监测区域内的最小分布密度，如果节点具备移动能力，还需要设计算法控制节点进行移动。通过执行相关算法，节点应该能够自组织地对周围环境自适应地完成对整个网络的部署。

6.1.1 网络覆盖问题概述

覆盖和连通是衡量无线传感器网络服务质量的主要指标之一。这是由于每个节点的感知范围相当有限，覆盖和连通衡量了多个节点协作形成的传感器网络的整体感知和通信能力。覆盖要求无线传感器网络能够以足够的精度感知监测区域中的每一点，而连通则要求相邻网络节点的数据传输保持畅通。对于随机抛撒部署的无线传感器网络，由于无法按照预先规划确定地放置节点，因此，需要设计网络初始化算法，对于分簇型无线传感器网络，如何在保证区域覆盖的前提下分簇、规划簇内节点数目、选择簇头，以有效保证覆盖和连通就变得尤其重要。

无线传感器网络覆盖问题所包含的基本要素如下：

(1)传感器节点布置方法。包括确定型和随机型。在大部分环境中可以采用确定型传感器节点布置方法；但对于军事应用和其他恶劣环境而言，则应采用随机型传感器节点的布置方法。

(2)感知和通信范围。感知和通信范围可能相同也可能不同，应针对感知范围和通信范围的特点和能力，选用合适的覆盖方法。

(3)应用需求。覆盖问题除了需要扩大网络覆盖范围外，还应确保网络覆盖的能量有效性和连通有效性。

(4)算法特性。网络覆盖算法包括集中式和分布式两种。在分布式算法的决策过程中，各节点仅利用临近节点的信息实现局部决策。由于无线传感器网络具有动态拓扑结构，且网络中包含大量传感器节点，因此，在无线传感器网络中应该采用分布式算法和协议，以提高算法的灵活性。

(5)特定目标。无线传感器网络覆盖问题的目标通常为最大化网络工作寿命或最小化网络节点数量。

近年来，国内学者对无线传感器网络覆盖控制问题进行了较为全面的研究[1~3]，着重分析了一些典型的无线传感器网络覆盖控制算法和协议，并提出了一些覆盖控制问题的思想和有代表性的研究成果，表 6.1 和表 6.2 列出了目前 5 种基本要素所对应的一些方法。

表 6.1　覆盖方法的基本要素

覆 盖 方 法	覆盖类型	对 应 目 标
最大约束—最小约束启发算法	区域覆盖	能源有效性;通过减少工作节点的数量最大化网络生命周期
分离支配集群启发算法	区域覆盖	
网络节点自规划算法	区域覆盖	
基于探针的密度控制算法	区域覆盖	能源有效性;通过控制节点的密度,最大化网络工作时间
最优地理密度控制算法	区域覆盖	能源有效性;连通性;通过减少工作节点的数量最大化网络工作时间
覆盖结构协议	区域覆盖	
基于连通支配集群的覆盖算法	区域覆盖	
网络节点布置算法	区域覆盖	能源有效性;连通性
	点覆盖	最小化传感器节点数量
分离集群覆盖启发算法	点覆盖	能源有效性;通过减少工作节点的数量最大化网络生命周期
最大化突破路径和最大化支持路径算法	边界覆盖	最差和最优覆盖路径
最大化支持路径算法	边界覆盖	最优覆盖路径
基于网络节点密度的覆盖算法	边界覆盖	寻找临界节点密度,但节点密度高于该值时,则肯定存在突破路径
最小化暴露路径算法	边界覆盖	寻找暴露可能性最小的路径
感知时间模型中完全覆盖的临界节点密度	边界覆盖	寻找目标监测的临界密度

表 6.2　覆盖方法的特性

传感器节点布置方法	感知范围/通信范围		算法特性	覆 盖 方 法
	各传感器节点感知范围是否相同	各节点感知范围与通信范围是否相等		
随机	是	—	集中式	最大约束—最小约束启发算法
随机	是	—	集中式	分离支配集群启发算法
随机	是	—	分布式	网络节点自规划算法
随机	是或否	—	分布式	基于探针的密度控制算法
随机	是	否	分布式	最优地理密度控制算法
随机	是	否	分布式	覆盖结构协议
随机	是	是	分布式	基于连通支配集群的覆盖算法
确定	是	否	集中式	网络节点布置算法
随机	是	—	集中式	
随机	—	—	集中式	分离集群覆盖启发算法
随机	—	—	分布式	最大化突破路径和最大化支持路径算法
随机	—	—	集中式	最大化支持路径算法
随机	—	—	集中式	基于网络节点密度的覆盖算法
随机	—	—	集中式	最小化暴露路径算法

若已知传感器节点的通信距离,可以通过文献[1]提出的方法得知所需配置的节点数,然后选择适当的感知半径。同样,如已确定传感器节点感知半径,可以先计算出布置的节点数,然后选择合适的通信距离或调整控制传感器节点功率大小。在通信距离和感知覆盖半径都确定的情况下,只有增加或减少节点数量来满足给定的最低连通可靠性和成本设计要求。

6.1.2　网络连通问题概述

在典型的无线传感器网络应用当中,传感器节点放置或配置除了要覆盖监测区域或点集外,通常需要配置的传感器集合能够形成一个互联的网络。对于已经放置好的传感器,很容易地就能检测是否配置的传感器集合覆盖了目标区域或点集,而且也能判断是否该集合的相互连通性。

对于无线传感器网络连通性设计而言,通常会遇到两个关键问题:一是在给定布置区域大小和节点无线通信半径的条件下,究竟要布置多少个节点才能连通一个网络,且连通的可靠性能满足多大的需求;二是给定节点感知距离半径的条件下,如何布置网络节点才能实现对给定区域的有效覆盖和监测。

由于连通性与功率和数据传输率有密切关系,为解决这两大问题,Gupta 和 Kumar 对无线网络的渐进连通性(趋近全连通)做了深入的研究[4],得出了临界发射传输功率与渐进全连通概率的关系模型,即随着通信半径不断增大,给定区域网络连通的概率存在一个 0 ~ 1 的阶跃跳变;当大于某个临界通信半径,网络连通的概率接近 1,如用晶格(Lattice)理论来解释的话,即深洞(Deep Holes)概率增加。由于 Gupta 和 Kumar 假设的模型是节点基于单位圆盘区域分布的,然而实际上很多无线传感器网络实际应用是带状或矩形区域。文献[5 ~ 8]分别从 Ad hoc 网络和小规模无线传感器网络方面做了一些探索工作,都是针对保持网络全连通分析所需要最小发射功率的研究。实际上,对于无线传感器网络很难做到网络完全连通,而且更关注连通的可靠性和保障机制以及覆盖的质量[9]。Jin Zhu 等对无线传感器网络连通性模型做了初步的研究,并考虑了无线传感器网络设计对功率和可靠性的折中,但没有对工程有关的网络连通概率、连通的可靠性和网络覆盖率做进一步的研究,进而提出一些实用的设计参考准则[10]。

6.1.3　覆盖与连通基本理论

【定义 6.1】覆盖:设 K 是线图 G 的一个顶点子集,如果 G 中每一条边至少有一个端点在 K 中,则称 K 为 G 的一个覆盖,集内顶点数最少的覆盖为最小覆盖。图 6.1 中的实点为该线图的一个最小覆盖。

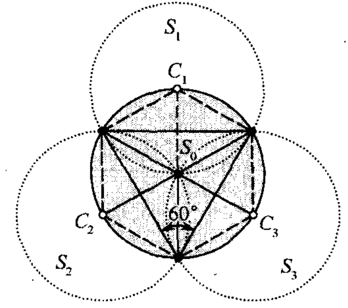


图 6.1　3 个圆实现的最小覆盖

【定义 6.2】连通:如果 i 个无缝拓扑圆域 $S_1,S_2,S_3,\cdots,S_i$ 相应的圆为 $C_1,C_2,C_3,\cdots,C_i$,且圆 $C_1,C_2,C_3,\cdots,C_i$ 的半径均为 r,$d_{C_1C_2},d_{C_2C_3},\cdots,d_{C_{i-1}C_i}$为圆心距,当满足:$d_{C_1C_2}\leqslant 2r,d_{C_2C_3}\leqslant 2r,\cdots,d_{C_{i-1}C_i}\leqslant 2r$ 时,则圆域 $S_1,S_2,S_3,\cdots,S_i$ 连通。

【定义 6.3】传感器网络拓扑结构:设图 $G(V,\ E)$是一

个传感器网络，$V(G)$是网络中所有节点(顶点)的集合，$V=\{v_1,v_2,\cdots,v_n\}$，v_n 表示网络中的某个节点；$E(G)$是网络中所有边的集合，$E=\{e_1,e_2,\cdots,e_n\}$，e_n 是网络的某个边，表示传感器网络系统中节点之间信息的传输关系或相互作用，则网络中节点与节点之间的连接方式(边)称为传感器网络拓扑结构。

【定义 6.4】关系矩阵：设在无向图 $G(V, E)$ 中，节点 v_i 的权为 ζ_i，边的权为 ω_{ij}，则网络的 n 阶关系矩阵为

$$\boldsymbol{Y}=\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} \\ b_{21} & b_{22} & \cdots & b_{2j} \\ \vdots & \vdots & \cdots & \vdots \\ b_{i1} & b_{i2} & \cdots & b_{ij} \end{bmatrix}, b_{ij}=\begin{cases}1, 若 v_i 与 v_j 相邻 \\ 0, 其他\end{cases} \quad (i, j=1,2,\cdots,n) \tag{6.1}$$

无线传感器网络的拓扑问题本质上是求图 $G(V, E)$ 的一个连通生成子图，使得在一定的约束条件及度量下性能最优[11]，在保证应用需求的前提下，使网络数据传输量最小，网络链路负载最小时的无线传感器网络拓扑结构数学模型为

$$H_{1\min}=\sum_{i=1}^{n}\sum_{j=i+1}^{n}\frac{F_{ij}}{I_{ij}-F_{ij}}\cdot J_{ij}+\sum_{i=1}^{n}\frac{O_i}{U_i-O_i} \tag{6.2}$$

$$H_{2\min}=W_{\mathrm{p}}\sum_{i=1}^{n}I_{ij}J_{ij}+W_{\mathrm{a}}\sum_{i=1}^{n}U_i \tag{6.3}$$

且

$$H_{3\min}=W_{\mathrm{p}}\sum_{i=1}^{n}F_{ij}J_{ij}+W_{\mathrm{a}}\sum_{i=1}^{n}O_i \tag{6.4}$$

并满足

$$F_{ij}\leqslant I_{ij}\leqslant \omega_{ij}, 1\leqslant j<i\leqslant n$$

$$O_{ij}\leqslant F_i\leqslant U_i, 1\leqslant i\leqslant n$$

$$\sum_{j=1}^{n}I_{ij}\leqslant F_i, 1\leqslant i\leqslant n$$

$$\sum_{j=1}^{n}a_{ij}\leqslant U_{ij}, 1\leqslant i\leqslant n$$

式中：H_1 为网络数据链路负载的大小程度；H_2 为网络数据帧设计流量处理代价；H_3 为网络数据帧实际流量处理代价；I_{ij}为网络节点 i 与节点 j 之间数据帧设计流量；F_{ij}为网络节点 i 与节点 j 之间数据帧实际流量；O_i 为网络节点 i 数据帧实际流量；U_i 为网络节点 i 数据帧设计流量；W_{p} 为网络节点处理单元感知数据的代价；W_{a} 为网络节点传输单元感知数据的代价；J_{ij}为节点 i 与节点 j 之间的连通关系，连通为 1，否则为 0。

该数学模型一方面可有效降低网络系统能耗，一方面可有效提高网络利用数据的实时性。

就覆盖特性而言，需要知道各个传感器节点的感应范围，设传感器节点能够感应距离 r 之内发生的事件，其中 r 为传感器的感应半径；就连通特性而言，需要知道传感器节点的

通信半径 c，H. Zhang 和 J. Hou 在文献[12]中给出了包含连通的覆盖的充分必要条件。

【定理 6.1】当传感器节点的密度，即单位区域的传感器节点的数目为有限时，$c \geqslant 2r$ 是覆盖包含连通性的充分必要条件。

X. Wang 等人[13]也证明了在 k 阶覆盖（每个点至少被 k 个传感器节点覆盖）和 k 阶连通性（配置传感器的通信图是 k 阶连接的）情况下的一个类似的结论。

【定理 6.2】当 $c \geqslant 2r$，一个凸区域的 k 阶覆盖必定包含了 k 阶连通性。

$k>1$ 的 k 阶覆盖提供了一定的容错度，只要不多于 $k-1$ 个传感器节点故障或失效，就能够监视所有的点。

6.1.4　网络连通可靠性

通常，无线传感器网络包括许多传感器节点，它们彼此通过多跳无线信道通信，而且通常都是要在没有预先准备情况下实现网络配置，以消耗尽可能少的能量来建立理想的通信拓扑，因此，采用适当的可靠性保证机制和性能更优的拓扑连通模型是十分必要的。

（1）网络连通度。无线传感器网络用连通概率来表示网络的连通性，而用每个节点邻居数不低于某个特定值来表示网络的连通可靠性需求。网络连通度是节点通信传输距离范围内的平均邻居节点数，邻居节点数越多，网络连通度越强。网络的连通性是和网络连通度成某种分布关系的。网络连通度（Connection Degree，CD）参数可反映网络的连通性。假设无线传感器网络是采用全向天线的同构网络，传输通信半径为 R，感知覆盖距离半径为 R'，网络配置区域为 $L \times W$ 的矩形带状区域，这样，CD 就集中反映了传感器节点数 n、实际物理布置区域大小以及每个节点的无线传输通信半径 R 三种因素的相互关系，D 表示节点密度，L 和 W 分别表示矩形域的长和宽。此外，无线网络特有的隐藏或暴露终端问题产生的节点干扰距离半径 R'（感知距离半径）通常满足条件 $R<R'<2R$，即

$$CD = \left(\frac{n}{LW}\right)\pi R^2 = D\pi R^2 \tag{6.5}$$

网络连通度和同频干扰会随着网络节点数增加而增强，同样，增大通信距离范围或减小网络布置区域大小，也会增大网络连通度和同频干扰。因此，选择适当的网络连通度对网络性能十分重要。

（2）网络冗余度。网络冗余度是无线传感器网络可靠连接的另一个重要参数。不考虑链路相互干扰等情况，冗余度 K 越高，网络的连通性越强。从几何拓扑学角度定义，网络冗余度是指在无穷维节点阵列空间连通的链路节点比（Link-to-node Ratio）。图 6.2(a) 中表示连通性最弱的冗余度 $K=1$，如一个环状或线性网络。网格网络冗余度可以是 $K=1.5,2,3,4$ 等，如图 6.2(b)～图 6.2(e)所示。

网络连通可靠性是无线传感器网络稳定运行必须面临的基本问题，通常有两种主要的理论研究与设计方法：一是基于图论的连通性；二是基于扩散理论的连通性。

1. 基于概率和图论的连接可靠性

图论中，根据图顶点之间边的连通情况将图分为有向图和无向图两种。无向图是指在图的顶点与顶点之间存在的边是无向边。由于网络拓扑的不确定性，无线传感器网络可以抽象成一个随机的无向图 $G_p(n)$。其中，n 为图中的顶点数（无线传感器网络的节点数），p 为任意两个节点之间的连通概率。在随机无向图 $G_p(n)$ 中，链路之间的连通是相

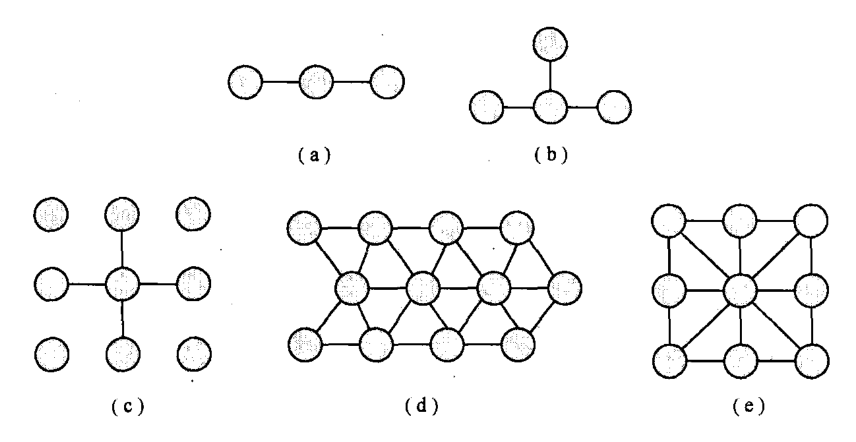


图 6.2　冗余度与网络连通性

(a)$K=1$; (b)$K=1.5$; (c)$K=2$; (d)$K=3$; (e)$K=4$。

互独立的事件。节点的度服从二项分布[14]，即

$$P_r[d=k]=\binom{n-1}{k}p^k(1-p)^{n-1-k}\approx\frac{z^k e^{-z}}{k!} \tag{6.6}$$

式中：z 为平均节点度，即 $z=E[d]=(n-1)p$。

在研究无线传感器网络连通性时，可将任意时刻的网络形式看做固定的拓扑图。如果图中任意两个节点之间存在 k 个相互独立的路径相连通，则称该图为 k 阶连通图。对于无线传感器网络而言，有如下定理。

【定理 6.3】将无线传感器网络看做 n 个顶点和 0 个边的图，任意并独立地逐一加入边，直至达到 m 条边，当满足条件 $m\geqslant n\times\lg(n)/2+O(n)$ 时，则无线传感器网络是全连通的。

定义 $p=\dfrac{m}{\binom{n}{2}}$，当满足条件 $p\geqslant\dfrac{\lg(n)}{n}$ 时，无线传感器网络是全连通的。

无线传感器网络的连通性依赖于节点的密度和传感器节点的通信感应半径。增加节点密度和感应半径将会增加节点的度。

【定理 6.4】对于节点数较多的无线传感器网络($n\geqslant 1$)，如感应半径为 r_0，节点分布密度为 ρ，则无线传感器网络图为 k 阶连通图的概率为

$$P_{r_0}[G\text{是}k\text{阶连通}]=P_{r_0}[d_{\min}\geqslant k] \tag{6.7}$$

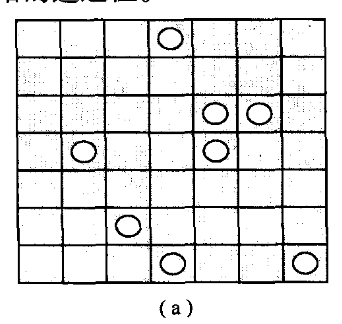
且同时有

$$P_{r_0}[d_{\min}\geqslant k]=\left(1-\sum_{N=0}^{k-1}\frac{(\rho\pi r_0)^N}{N!}e^{-\rho\pi r_0}\right)^n \tag{6.8}$$

2. 基于扩散理论的连通可靠性

图 6.3 是由许多正方形网格组成的区域 Z^2，每个网格随机被网络节点占据，网格被占据的概率为 p，在整个区域内会形成许多网络簇，簇是由相邻的被网络节点占据的网格组成，相邻的网格之间有一条公共边。扩散理论(Percolation)就是对簇的数目和特性进行研究的理论[13]，在图 6.3 中，如果两个节点属于相同的簇，则它们之间能够进行通信。

如果网络中大多数节点都属于相同的无限大的簇,则网络具有较好的连通性。如果无线传感器网络中存在无限大小的簇,则称为扩散现象。因此,扩散理论可以很好地用来研究无线传感器网络的连通性。


(a)

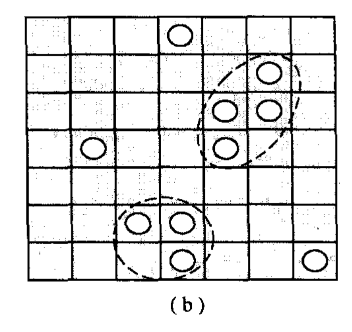

(b)

图 6.3　扩散簇的形成

(a)网络节点填充网格;(b)网络节点形成簇。

关于扩散理论有以下两个基本理论模型。

1)布尔模型

节点按照泊松点过程分布,当两个节点间的距离小于等于发射半径时,能够相互连通。因此,在一维网络中,如泊松分布过程为半径是 $r/2$ 的圆中心,两节点间的距离按指数分布,则不存在扩散现象。当给定 r 和 λ 时,距离为 x 的两节点连通概率为

$$P_c(x) = \sum_{i=0}^{\left\lfloor \frac{x}{r} \right\rfloor}\left(\frac{-\lambda e^{-\lambda r}(x-ir)^i}{i!}\right) - e^{-\lambda r}\sum_{i=0}^{\left\lfloor \frac{x}{r} \right\rfloor-1}\left(\frac{-\lambda e^{-\lambda r}(x-(i+1)r)^i}{i!}\right) \leqslant \exp(-\lambda(x-r)e^{-\lambda r}) \tag{6.9}$$

由式(6.9)可知,随着 x 的增加,两节点间的连通概率按指数规律下降。

若在二维网络中,有如下定理。

【定理 6.5】对于给定的 r,存在临界的节点密度 λ^*,且当节点密度 $\lambda \leqslant \lambda^*$ 时,网络由无限个有线簇组成,即网络不连通;当节点密度 $\lambda > \lambda^*$ 时,网络由唯一的无限簇组成,则网络全连通。

2)STIRG 模型

扩散理论中,信噪比图模型 STIRG(Signal to Interference Radio Graph)定义为,若节点 j 收到从节点 i 发送的信号信噪比大于某个阈值 β,则节点 j 将能接收到从节点 i 发送来的数据

$$\frac{P_i l(\|x_i - x_j\|)}{N_0 + \gamma \sum P_k l(\|x_k - x_j\|)} \geqslant \beta \tag{6.10}$$

式中:γ 为干扰因子;N_0 为热噪声。

(1)当 $\gamma = 0$ 时,即无干扰的情况下,节点能与某一个固定范围内的节点进行通信(与节点发射功率有关),则存在临界节点密度 λ^*(与布尔模型相同)。

(2)当 $\gamma \neq 0$ 时,由于存在干扰,网络图中会形成许多节点数目较少的簇,从而导致网络不连通或连通较差。因此,干扰因子 γ 存在临界值 γ^*。

(3)当$0\leq\gamma^*<\frac{1}{\beta}$时,则可能存在扩散现象。

(4)当$\gamma^*>\frac{1}{\beta}$时,无论节点密度如何,网络中不存在扩散现象,即网络不连通。

6.2　无线传感器网络覆盖与连通模型

分簇方案设计的主要问题之一是应该形成多少个簇,在传感器网络中由于簇头节点比传感节点消耗更多的能量,因此簇头节点数量最小化十分重要。并且为了使有限的传感器网络节点能够完成一定区域内的监测任务,需要通过一定的算法来合理地部署簇头节点,优化网络资源,以期在应用中获得最大的利用率。传感器网络的能耗与簇头节点位置分布有关,文献[16]中证明了簇头节点均匀分布的能耗最小的结论。

本节采用几何学和图论覆盖与连通理论的思想,在文献[16]的基础上研究了无线传感器网络系统的连通与覆盖的 3 种数学模型,并给出了适合智能监测拓扑结构的无线传感器网络区域 3 种网格划分方法。

6.2.1　覆盖与连通模型

设给定的传感器区域为$S(L*W)$,且满足定义 6.3 和 6.4 的前提下,得到如图 6.4 所示的 3 种连通与覆盖模型:图 6.4(a)体现了在保证连通和覆盖的情况下,节点数量最少,但要求 Sink 节点通信半径必须能够覆盖整个监测区域;图 6.4(b)体现了连通情况下,节点数有所增加,覆盖面积较图 6.4(a)有所增加,但在不要求 Sink 节点通信半径必须能够覆盖整个监测区域前提下,保证了簇头节点到 Sink 节点通信链路的连通性;图 6.4(c)体现了连通的情况下,节点数量最大,覆盖面积也较图 6.4(a)和图 6.4(b)大,在不要求 Sink 节点通信半径必须能够覆盖整个监测区域前提下,增加了相邻簇头节点的通信链路数量。

3 种连通与覆盖模型分别描述如下。

1. 模型一:Sink 节点可以完全覆盖整个区域$S(L\times W)$簇头节点的放置机制

【**定理 6.6**】圆的内接三角形中等边三角形的面积最大。

【**定理 6.7**】如果 3 个无缝拓扑圆域S_1,S_2,S_3相应的圆C_1,C_2,C_3相交于一点S,且$\Delta C_1C_2C_3$为等边三角形,则 3 个圆域的无缝拓扑面积为最大,即$\max(S_1\cup S_2\cup S_3)$,也即$S_1,S_2,S_3$是连通的,如图 6.4(a)所示。

依据定理 6.6、定理 6.7 和图 6.4(a)划分网格,具体规则如下:

(1)作一条距底边界$R/2$处且与底边界平行的辅助线,辅助线与左边界的交点为K,以K为起点,以$\sqrt{3}R$为线段长度等分该辅助线,并分别以等分点为起点,以夹角 60°和 60°作射线直到和区域边界相交。

(2)以K为起点,以$3R/2$为线段长度等分左边界,分别以等分点为起点作与底边界平行的射线直到与右边界相交,这样就将整个区域划分成如图 6.5 所示的三角形网格,各个三角形的顶点则为簇头节点的位置。这样,无线传感器网络就实现了完全无缝连通。由划分簇的过程得到

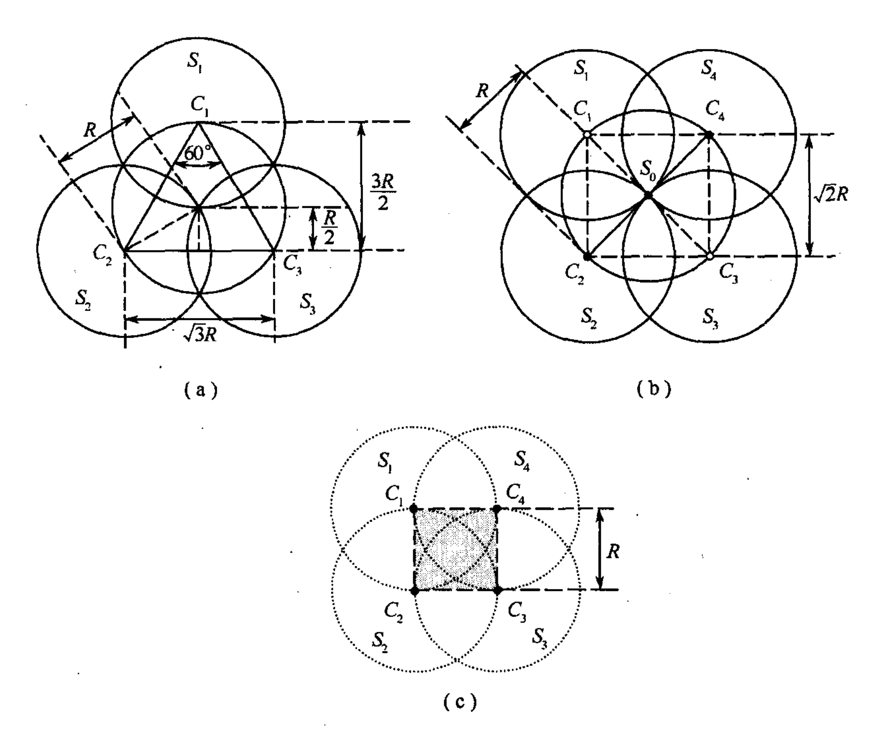


图 6.4 3 种连通与覆盖模型

$$N_C = \left\lceil \frac{L}{\sqrt{3}R} \right\rceil \times \left\lceil \frac{W - R/2}{3R/2} \right\rceil \tag{6.11}$$

式中:N_C 为最小簇头节点数量;L 为监测区域长度;W 为监测区域宽度;R 为簇头节点通信半径;[*]为不小于 * 的最小整数。

式(6.11)就是无线传感器网络所需划分的最小覆盖的簇头节点数公式。

(3)同理,可得到无线传感器网络最小覆盖的传感节点数为

$$N_S = \left\lceil \frac{L}{\sqrt{3}r} \right\rceil \times \left\lceil \frac{W - r/2}{3r/2} \right\rceil \tag{6.12}$$

式中:N_S 为最小传感节点数量;r 为传感节点通信半径。

经过以上的网格划分过程,得到如图 6.5 和图 6.6 所示的无线传感器网络实现完全无缝连通和完全无缝覆盖模式,该模式下网络系统消耗的能量是较低的。

2. 模型二:Sink 节点无法覆盖整个区域 $S(L \times W)$,且通信半径大于等于传感节点与簇头节点的通信半径,簇头节点的放置机制

虽然簇头节点已经连通且覆盖监测区域,但 Sink 节点通信半径无法覆盖整个监测区域,部分簇头将无法直接与 Sink 节点通信,因此在定义 6.3 和 6.4 的前提下,依据图 6.4(b)划分网格,具体规则如下:

(1)作一条距底边界 R 处且与底边界平行的辅助线,辅助线与左边界的交点为 K,以 K 为起点,以$\sqrt{2}R$ 为线段长度等分该辅助线,并分别以等分点为起点,以夹角 45°和 135°作射线直到和区域边界相交。

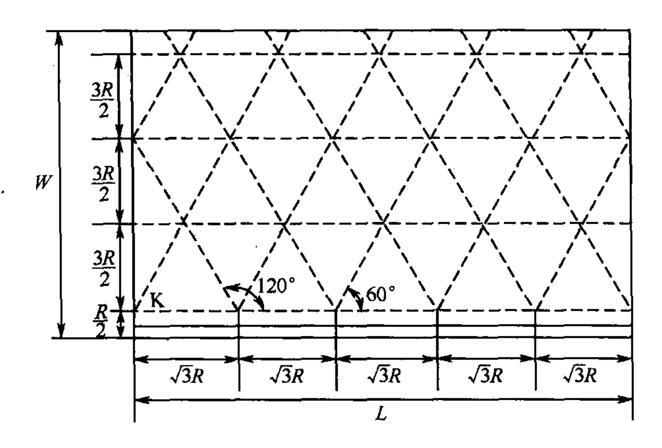


图 6.5　模型一的簇头节点放置图

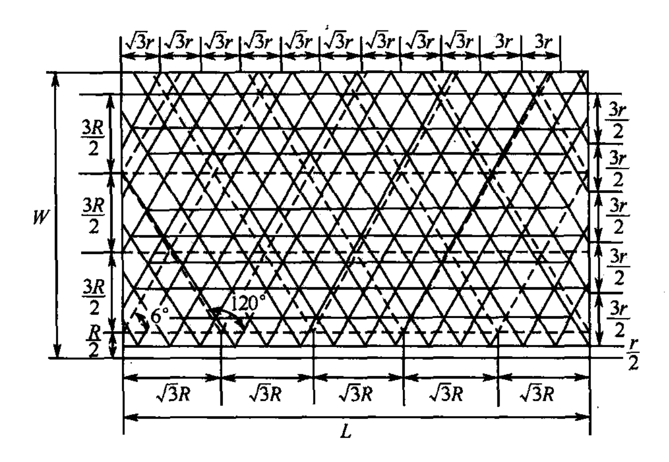


图 6.6　模型一的簇头节点与传感节点放置图

(2)以 K 为起点,以$\sqrt{2}R$ 为线段长度等分左边界,分别以等分点为起点作与底边界平行的射线直到与右边界相交,这样就将整个区域划分成如图 6.7 所示的三角形网格,各个三角形的顶点则为簇头节点的位置。

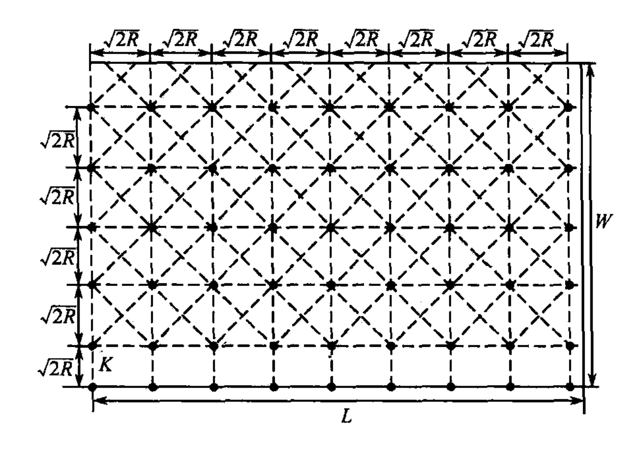


图 6.7　模型二的簇头节点放置图

这样，在不要求 Sink 节点通信半径必须能够覆盖整个监测区域前提下，保证了簇头节点到 Sink 节点通信链路的连通性，实现了无线传感器网络完全无缝连通。由划分簇的过程得到

$$N_C = \left[\frac{L}{\sqrt{2}R}\right] \times \left[\frac{W-R}{\sqrt{2}R}\right] \tag{6.13}$$

3. 模型三：Sink 节点无法覆盖整个区域 $S(L \times W)$，且通信半径大于等于传感节点与簇头节点的通信半径，相邻簇头节点的通信链路数量增加了的簇头节点的放置机制

虽然簇头节点已经连通且覆盖监测区域，但 Sink 节点通信半径无法覆盖整个监测区域，部分簇头将无法直接与 Sink 节点通信，模型二中尽管簇头节点可以将信息路由到 Sink 节点，但簇头节点的相互通信链路较少，因此在定义 6.3 和 6.4 的前提下，依据图 6.4(c)划分网格，具体规则如下：

(1)以左边界顶点 K 为起点，以 R 为线段长度等分左边界，并分别以等分点为起点，作与底边界平行的射线直到与右边界相交。

(2)以 K 为起点，以 R 为线段长度等分下边界，分别以等分点为起点作与左边界平行的射线直到与上边界相交，这样就将整个区域划分成如图 6.8 所示的正方形网格，各个正方形的顶点则为簇头节点的位置。

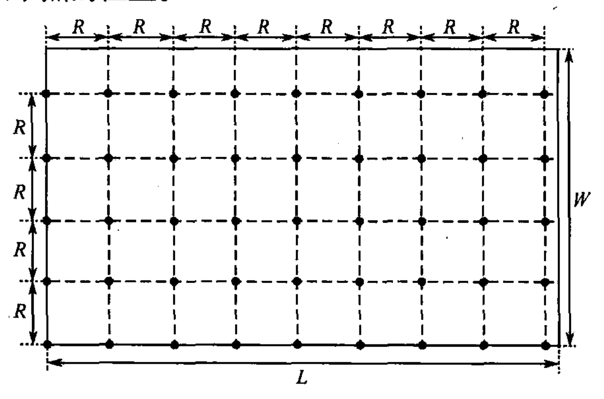


图 6.8　模型三的簇头节点放置图

这样，在不要求 Sink 节点通信半径必须能够覆盖整个监测区域前提下，保证了簇头节点到 Sink 节点通信链路的连通性，增加了相邻簇头节点的通信链路数量，实现了无线传感器网络完全无缝连通。由划分簇的过程得到

$$N_C = \left[\frac{L}{R}\right] \times \left[\frac{W}{R}\right] \tag{6.14}$$

6.2.2　网络节点数目计算

应根据具体应用需求，确定无线传感器网络监测区域范围和监测对象的具体情况。根据监测范围的大小和监测参数的数量、计算网络节点数量，即传感节点和簇头节点的数量，由于 Sink 节点只有一个，因此根据应用需求其通信半径有可能远离监测区域。

(1)保证至少有一个簇头节点在 Sink 节点的通信范围内。

(2)如果没有簇头节点在 Sink 节点的通信半径内，可通过增加簇头节点中继的方法

实现无线传感器网络的连通。簇头节点和传感节点的数量直接关系到整个网络的成本和性能，并将影响通信协议的设计。在本文设计的无线传感器网络原型中，簇头节点已知，簇头节点与传感节点属于异构节点，因此，在连通与覆盖的基础上，区域 $S(L*W)$ 内网络所需最少活动节点的总数为

$$N = N_C + N_S \tag{6.15}$$

(3)设无线射频芯片的最大数据传输率为 100Kb/s，设传感节点采样频率为 F_s，传感节点的传感器信道数量为 s，采样值为 b，传感节点的数据产生率为 K_s，则 $K_s = F_s \times s \times b$，设信道吞吐量为 75%，那么，必有下式成立才能保证数据的有效通信：

$$\frac{K_s \times (N_S + 1) \times (N_C + 1)}{0.75^2} \leqslant 100 \tag{6.16}$$

6.2.3　覆盖率计算

分布式监测要求区域中的每个位置至少被一个传感节点覆盖，对于分布式跟踪及目标识别的网络应用，则要求每个位置至少被 k 个传感节点覆盖。分簇型无线传感器网络中，每个簇负责一个监测区域，当簇内成员节点较多时，可在满足覆盖率的前提下，让部分节点处于低能耗休眠状态；当覆盖率不满足要求时，这些节点转入工作状态。

覆盖率主要关心在半径为 R 的簇区域 D 中，需要布置多少个感知半径为 $R_s(R_s \leqslant R)$ 的节点，以保证区域以一定概率被网络覆盖。为描述方便，令簇区域 D 的圆心坐标为(0,0)，并作如下定义。

【定义 6.5】邻域。对于任意坐标为 $(x,y) \in D$ 的点，其邻域定义为

$$N(x,y) = \{(x',y') \in D \mid (x'-x)^2 + (y'-y)^2 \leqslant R_s^2\} \tag{6.17}$$

对于 $\forall (x,y) \in D$，如果在其邻域内至少有一个节点，则该点被覆盖。因为区域 D 中节点随机均匀分布，节点落入点 (x,y) 邻域的概率为

$$p = \frac{|N(x,y)|}{|D|} = \frac{R_s^2}{R^2}$$

若某个簇区域 D 中有 n 个成员节点，则点 (x,y) 被单重覆盖的概率为

$$P_{\text{single-cover}} = C_n^1 p(1-p)^{n-1} + C_n^2 p^2 (1-p)^{n-2} + \cdots + C_n^n p^n = \sum_{i=1}^{n} C_n^i p^i (1-p)^{n-i} \tag{6.18}$$

对于 k 重覆盖 $(k \leqslant n)$，簇中任意一点的邻域内至少有 k 个节点。因此，簇区域 D 被节点 k 重覆盖的概率为

$$\begin{aligned} P_{k\text{-cover}} &= C_n^k p^k (1-p)^{n-k} + C_n^{k+1} p^{k+1} (1-p)^{n-k-1} + \cdots + C_n^n p^n \\ &= \sum_{i=1}^{n} C_n^i p^i (1-p)^{n-i} \end{aligned} \tag{6.19}$$

图 6.9(a)和图 6.9(b)是区域半径 R = 20m，节点感知半径分别为 5m、6m、10m 和 15m 时，单重覆盖率及二重覆盖率与簇内节点数的关系。从图上看出，对于相同的感知半径，节点数越多，覆盖率越高；对于相同节点数目，感知半径越大，覆盖率也越高；感知半径

和节点数目相同时，单重覆盖率大于二重覆盖率。

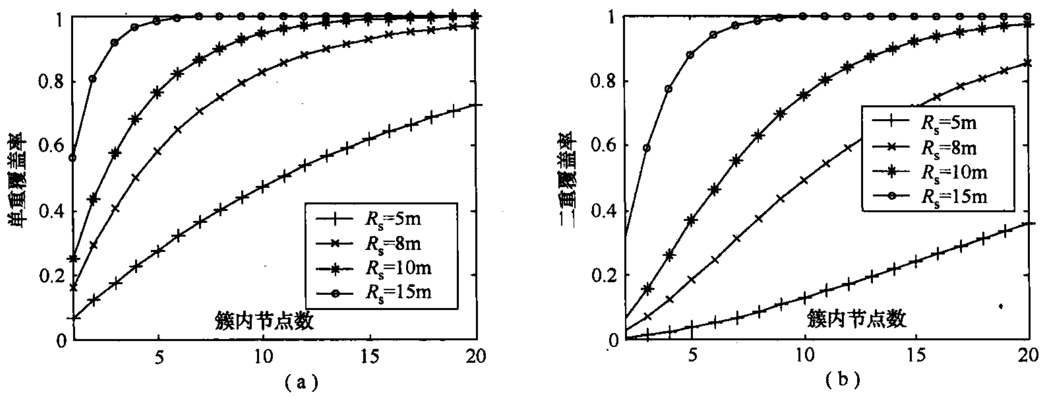


图 6.9　簇内覆盖率与通信半径及节点数关系

6.3　最优分簇数目

簇数目的多少影响网络能耗和相关协议的性能，本章在网络能耗模型的基础上，推导了簇头数据聚集能力不受限和受限两种情形下的最优分簇数目。

分簇算法主要研究通过何种方式将节点划分为簇，使簇数目与最优分簇数目一致。现有的分簇算法大都只关心算法的消息和计算复杂度，难以保证簇数目的最优和簇内节点的均匀性。本章通过模糊 C 均值聚类算法进行分簇，当聚类中心数与最优分簇数目一致时，既保证了分簇数与最优分簇数目相同，又使簇内节点数具有较好的均匀性，避免某个簇内节点数过多或过少，引起能耗不均衡。

分簇型网络在自组织过程中，将网络分为多少个簇是需要解决的首要问题。簇数目过多或过少都会引起性能下降：过多的簇不便于 Sink 管理，也会导致和 Sink 直接通信的节点数增多，增大远距离通信能耗；簇数目过少，簇内成员节点数目过多，又会增加簇头的管理难度，进而影响簇内 MAC 协议或数据聚集算法的性能。本节在能耗模型的基础上，针对簇头聚集能力不受限和受限两种情形，研究随机布置网络的最优分簇数目。

6.3.1　节点能耗模型与基本假设

1. 节点能耗模型

1）节点发送数据包能耗模型

传感器节点之间依靠 RF 信号进行无线通信，发送数据包的能耗包括发射电路能耗 $E_{Tx-elec}(l)$ 和放大电路能耗 $E_{Tx-amp}(l,d)$ 两部分，如图 6.10 所示。

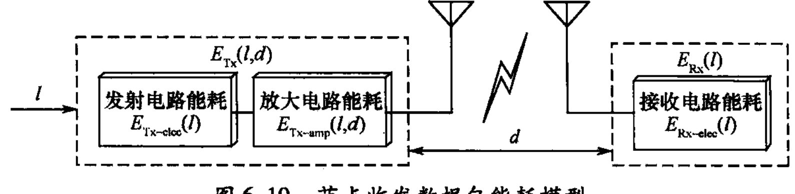


图 6.10　节点收发数据包能耗模型

根据发送节点和接收节点的距离 d 与阈值距离 d_0 的关系，节点发送数据包能耗模型有自由空间模式和多径衰减模式两种：当 d 小于 d_0 时，选择自由空间模式；当 d 大于或等于 d_0 时，采用多径衰减模式。因此，节点将长度为 l 的数据包发送至距离为 d 处节点的能耗为

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & (d < d_0) \\ lE_{elec} + l\varepsilon_{amp}d^4 & (d \geq d_0) \end{cases} \tag{6.20}$$

式中：E_{elec}、ε_{fs}、ε_{amp} 为常数，由实际节点性能决定。

2）节点接收数据包能耗模型

节点接收数据包时，只有接收电路工作，因此节点接收长度为 l 的数据包的能耗为

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \tag{6.21}$$

3）簇头数据聚集能耗模型

簇头将 n 个长度为 l 的成员节点数据包聚集为一个长度为 l 的数据包的能耗为

$$E_{aggregation}(n,l) = nlE_{DA} \tag{6.22}$$

式中：E_{DA} 为聚集 l 数据包的能耗。

4）传感器节点感知能耗模型

节点中的传感器模块、ADC 和 MCU 共同采集长度为 l 的感知数据能耗为

$$E_{sense}(l) = lE_{sense} \tag{6.23}$$

式中：E_{sense} 为采集和处理 l 感知数据包的能耗。

2. 基本假设

（1）N 个节点随机均匀分布在边长为 M 的方形区域中。

（2）簇头均匀分布，即每个簇内的成员节点数目近似相等。

（3）对 Sink 而言，节点位置已知。

（4）节点的通信半径不小于感知半径的 2 倍，网络满足覆盖与连通要求。

（5）所有节点之间可靠通信，不存在恶意攻击的节点。

（6）节点和簇头之间通信采用自由空间模式，簇头与 Sink 之间采用多径衰减模式。

图 6.11 为 200 个节点随机均匀分布在面积为 100×100区域内的示意图。

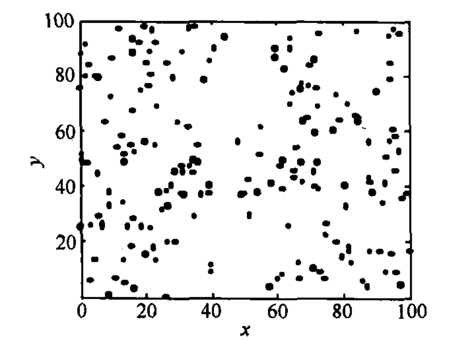


图 6.11　节点随机分布示意图

6.3.2　簇头聚集能力不受限时的最优分簇数目

当簇头有足够的数据聚集能力时，簇头可将成员节点和簇头自身的感知数据一次性的聚集为一个长度固定的数据包，并转发至 Sink。

若监测区域内的 N 个节点被均匀划分为 k 个簇，每个簇内的节点数为 $\frac{N}{k}-1$，根据节点能耗模型可知：簇头能耗包括接收簇内节点感知数据的接收能耗、数据聚集能耗和向 Sink 转发数据的发送能耗 3 个部分；成员节点能耗包括数据感知能耗和向簇头发送数据包能耗。簇头能耗 E_{CH} 和节点能耗 E_{membe} 具体形式为

$$E_{\mathrm{CH}} = \left(\frac{N}{k}-1\right)lE_{\mathrm{elec}} + lE_{\mathrm{DA}}\frac{N}{k} + (lE_{\mathrm{elec}} + l\varepsilon_{\mathrm{amp}}d_{\mathrm{toBS}}^4) \tag{6.24}$$

$$E_{\mathrm{member}} = lE_{\mathrm{elec}} + l\varepsilon_{fs}d_{\mathrm{toCH}}^2 \tag{6.25}$$

式中：d_{toBS} 为节点与簇头的距离；d_{toCH} 为簇头与 Sink 的距离。

由式(6.24)与式(6.25)可得，一个簇内所有节点总能耗(包括簇头)为

$$E_{\mathrm{cluster}} = E_{\mathrm{CH}} + \left(\frac{N}{k}-1\right)E_{\mathrm{member}} \approx E_{\mathrm{CH}} + \frac{N}{k}E_{\mathrm{member}} \tag{6.26}$$

则整个网络的总能耗为：

$$\begin{aligned} E_{\mathrm{total}} &= kE_{\mathrm{cluster}} \approx NE_{\mathrm{member}} + kE_{\mathrm{CH}} = \\ &N(lE_{\mathrm{elec}} + l\varepsilon_{\mathrm{fs}}d_{\mathrm{toCH}}^2) + (N-k)lE_{\mathrm{elec}} + lE_{\mathrm{DA}}N + k(lE_{\mathrm{elec}} + l\varepsilon_{\mathrm{amp}}d_{\mathrm{toBS}}^4) = \\ &l(2NE_{\mathrm{elec}} + N\varepsilon_{\mathrm{fs}}d_{\mathrm{toCH}}^2 + E_{\mathrm{DA}}N + k\varepsilon_{\mathrm{amp}}d_{\mathrm{toBS}}^4) \end{aligned} \tag{6.27}$$

由于节点在监测区域内是随机均匀分布的，簇内的节点也服从均匀分布。每个簇占据的区域 D 可用以簇头为圆心，等效半径 $r = M/\sqrt{k\pi}$，面积为 M^2/k 的圆形近似表示。在第 i 个簇占据的区域 D_i 内，以簇头为原点，建立如图 6.12 所示的坐标系。

若区域 D_i 内某个节点 S 的位置为 (x,y)，则节点分布密度函数为

$$\rho(x,y) = \begin{cases} \dfrac{k}{M^2} & (x,y \in D_i) \\ 0 & (x,y \notin D_i) \end{cases} \tag{6.28}$$

图 6.12　簇内区域的等效

该节点与簇头距离平方的数学期望为

$$E[d_{\mathrm{toCH}}^2] = E[x^2+y^2] = \iint_{D_i}(x^2+y^2)\rho(x,y)\,\mathrm{d}x\mathrm{d}y = \frac{M^2}{2k\pi} \tag{6.29}$$

从 $E[d_{\mathrm{toCH}}^2]$ 的形式来看，簇数目 k 越大，节点与簇头距离的数学期望越小，节点向簇头发送数据包的能耗就越少；反之，节点与簇头距离的数学期望越大，节点向簇头发送数据包的能耗就越多。但簇数目 k 增多，簇头数目也相应增加，进行长距离通信的能耗也相应增加。

将式(6.29)代入式(6.28)，得网络总能耗为

$$E_{\mathrm{total}} = l\left(2NE_{\mathrm{elec}} + \frac{M^2}{2k\pi}N\varepsilon_{\mathrm{fs}} + E_{\mathrm{DA}}N + k\varepsilon_{\mathrm{amp}}d_{\mathrm{toBS}}^4\right) \tag{6.30}$$

图6.13为簇头至Sink的平均距离分别为90m和100m时，网络内节点总能耗与簇数目k的关系图，网络的其他参数如表6.3所列[①]。

表6.3　网络参数

参数名称	参数值	参数名称	参数值
节点数目N	100个	E_{elec}	50nJ/bit
区域边长M	100m	E_{DA}	5pJ/bit/signal
		ε_{fs}	10pJ/bit/m^2
数据包长度l	6bit	ε_{amp}	0.0013pJ/bit/m^4

当k增大时，总能耗先减小、后增加。图6.14是总能耗与k、d_{toBS}的曲面图，从图上看：对于相同d_{toBS}值，k增大时，总能耗先减小、后增加；对于相同的k值，d_{toBS}增大时，总能耗也增大。

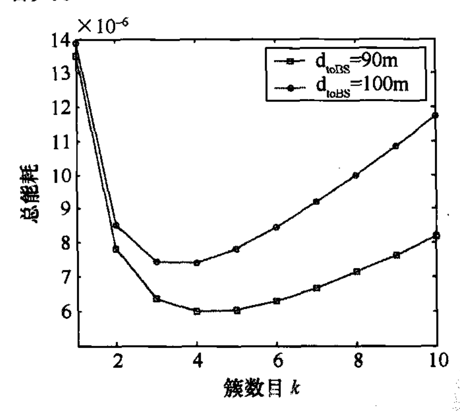


图6.13　总能耗与簇数目k的关系

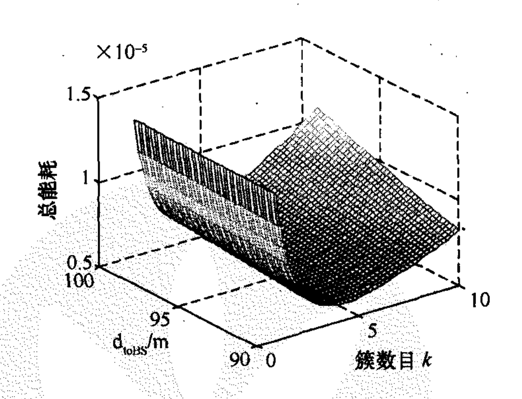


图6.14　总能耗与簇数目k、d_{toBS}关系

对式(6.30)关于k求一阶导数，得

$$\frac{\mathrm{d}E_{total}(k)}{\mathrm{d}k}=l\left(\varepsilon_{amp}d_{toBS}^4-\varepsilon_{fs}\frac{M^2}{2k^2\pi}N\right)\tag{6.31}$$

当$k_{opt}=\dfrac{M}{d_{toBS}^2}\sqrt{\dfrac{N\varepsilon_{fs}}{2\pi\varepsilon_{amp}}}$时，$\dfrac{\mathrm{d}E_{total}(k)}{\mathrm{d}k}=0$，网络总能耗$E_{total}$最小。此时的$k$值即为簇头数据聚集能力不受限时，网络内节点总能耗最小的最优分簇数目。

由于整个网络占据的区域为方形，且Sink位于监测区域中心位置，这样才方便计算簇头与Sink距离平方的数学期望。当Sink位于监测区域外部或非中心位置时，需重新计算簇头与Sink距离平方的数学期望。

6.3.3　簇头聚集能力受限时的最优分簇数目

当簇头处理能力有限，一次只能聚集m个($m\leqslant\dfrac{N}{k}$，m称为压缩比)长度为l的感知数据时，簇头需经$\dfrac{N}{km}$次才能将自身和成员节点的感知数据转发至Sink。此时，网络总能

① 表6.3中的参数参照Berkeley的Mica2节点性能参数。

耗为

$$E_{\text{total}} = l\Big[(2N-k)E_{\text{elec}} + \frac{M^2}{2k\pi}N\varepsilon_{\text{fs}} + E_{\text{DA}}N + \frac{N}{m}(E_{\text{elec}} + \varepsilon_{\text{amp}}d_{\text{toBS}}^4)\Big] \tag{6.32}$$

对式(6.32)关于 k 求一阶导数，得

$$\frac{\mathrm{d}E_{\text{total}}(k)}{\mathrm{d}k} = -l\Big(E_{\text{elec}} + \varepsilon_{\text{fs}}\frac{M^2}{2k^2\pi}N\Big) < 0 \tag{6.33}$$

由式(6.33)可知，在簇头数据聚集能力受限时，总能耗 $E_{\text{total}}(k)$ 为 k 的单调递减函数。

图 6.15 和图 6.16 为考虑簇头数据聚集能力时，网络总能耗与簇数目和簇头聚集能力 m 的关系图。显然，当 k 或 m 增大时，总能耗减小。因为簇数目 k 需满足 $k \leqslant \frac{N}{m}$，所以当 $k_{\text{opt}} = \frac{N}{m}$ 时，网络总能耗最小。

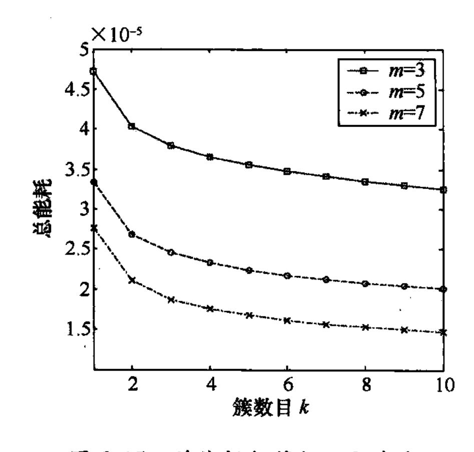


图 6.15　总能耗与簇数目 k 关系

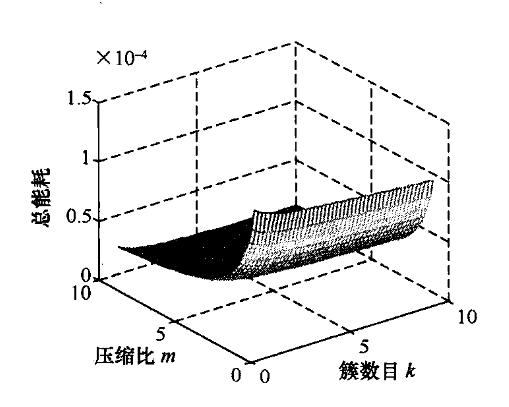


图 6.16　总能耗与 k、m 关系

根据上述分析，可得如下结论：

(1)对于由 N 个节点构成的分簇型无线传感器网络，若簇头的数据聚集能力 m 不受限，所有节点完成一次感知、收发和聚集的总能耗最小时，最优分簇数目 $k_{\text{opt}} = \frac{M}{d_{\text{toBS}}^2}\sqrt{\frac{N\varepsilon_{\text{fs}}}{2\pi\varepsilon_{\text{amp}}}}$；

(2)对于由 N 个节点构成的分簇型无线传感器网络，若簇头的数据聚集能力 m 受限，所有节点完成一次感知、收发和聚集的总能耗最小时，最优分簇数目 $k_{\text{opt}} = \frac{N}{m}$，且与区域边长、簇头至 Sink 的距离无关。

参 考 文 献

[1] 宋文，方旭明．基于连接与覆盖模型的无线传感器网络设计规划研究[J]．西南交通大学学报，2006.

[2] 任彦，张思东，张宏科．无线传感器网络中覆盖控制理论与算法[J]．软件学报，2006，17(3)：422－433.

[3] 孙永进,孙雨耕,房朝晖. 无线传感器网络连通与覆盖[J]. 天津大学学报,2005,36(1):14 – 17.

[4] Gupta R, Kumar R R. Critical Power for AsymPtotic Connectivity in Wireless Networks. Stochastic Analysis, Control, optimization and Applications[J]. Boston:Birkhauser, 1996:547 – 566.

[5] Santl P, Blough D M, Vainstein F. A Probabilistie analysis fortherangeassignment problem in ad hoc networks[C]. In: ACM M obiHoc'02. Long Beach:2001:26 – 220.

[6] Mehrotra Shashank. Distributed Algorithms for Tasking Large Sensor Network. Virginia:The Bradley Department of Electrical and Computer Engineering[C], Virginia Polyteehnie Institute and State University, 2001.

[7] Wu J. Extended Dominating – set – based Routing in Ad hoc Wireless Networks with Unidirectional Links[J]. IEEE Transactions on Parallel and Distributed Systems, 13(9):666 – 661, 2002.

[8] Dai F, Wu J. Distributed Dominant Pruning in Ad hoc Networks[C]. IEEE International Conference on Communications, 353 – 357 vol. 1,2003.

[9] Zhang H, Hou J. Maintaining Sensing Coverage and Connectivity in Large Sensor Networks. Wireless Ad Hoc and Sensor Networks[J]. An International Journal, 1(1 – 2):69 – 63, 2005.

[10] Jin Zhu , Papavassiliou S. On the Connectivity Modeling and the Tradeoffs between Reliability and Energy Efficiency in Large – scale Wireless Sensor Networks[C]. WCNC 2003, (2):16 – 20, March, 2003. 660 – 665.

[11] Ellen W Zegura, Kenneth L Calvert, Michael J Donahoo. A Quantitative Comparison of Graph – based Models for Internet Topology [J]. IEEE/ACM Transactions networking, 1997,5(6):770 – 763.

[12] Zhang H, Hou J. Maintaining Sensing Coverage and Connectivity in Large Sensor Networks[C]. Technical Report UIUC, UIUCDCS – R – 2003 – 2351,2003.

[13] Wang X, Xing G, Zhang Y, etc. Intergated Coverage and Connectivity in Wireless Sensor Networks[C]. In: Akyildia IF, Estion D, eds. Proc. of the ACM Int'l Conf. On Embedded Networked Senso Systems. New York: ACM Press, 2003:26 – 39.

[14] Bettstetter C. On the Minimum Node Degree and Connectivity of A Wireless Multihop Network[D]. In Proc. MobiHoc, Lausanne, Switzerland, June 2002.

[15] Grimmet G, Percolation, Springer – Verlag[M], Berlin, 1999.

[16] 郭忠文. 传感器网络关键算法研究[D]. 中国海洋大学, 2005.

第3篇

无线传感器网络组网协议

第7章 无线传感器网络物理层协议

无线传感器网络物理层需要承担为网络数据终端提供数据传输通路、传输数据和完成管理工作的职责。具体而言,就是介质的选择、频段的选择、调制技术以及扩频技术。无线传感器网络的传输介质主要为电磁波,源信号依靠电磁波传输需要通过调制技术变成高频信号,当抵达接收端时,又通过解调技术还原成原始信号。目前采用的调制方法分为模拟调制和数字调制两种,区别就在于调制信号所用的基带信号的模式不同。此外,经过调制的信号还需要进行扩频。扩频就是将待传输数据进行频谱扩展的技术。扩频的好处是增强了抗干扰能力、可进行多地址通信、保密性提高。常见的扩频技术包括直接序列扩频、跳频、跳时以及线性调频。

在物理层面上,无线传感器网络遵从的主要是 IEEE 802.15.4 标准。依照此标准,物理层主要进行如下工作:激活和去活无线收发器、检测当前信道的能量、发送指示、信道频率的选择、数据发送与接收。IEEE 802.15.4 标准规划了几个工作频段。其中,2.4GHz 频段的物理层可提供250Kb/s 的数据传输率,适用于高吞吐量、低延时或低作业周期的场合;工作在 867/715MHz 频段的物理层则能提供 20Kb/s 的数据传输率,适用于低速率、高灵敏度和大覆盖面积的场合。依据 IEEE 802.15.4 标准的协议被称为 ZigBee,其传输带宽虽然没有 Wi－Fi 和 Blue Tooth 大,但是能耗较低,非常适合无线传感器网络。

7.1 物理层概述

国际标准化组织(International Organization for Standardization,ISO)对开放系统互联(Open System Interconnection,OSI)参考模型中的物理层做了如下定义:在物理传输介质之间为比特流传输所需物理连接的建立、维护和释放提供机械的、电气的、功能的和规程性的手段[1,2]。

在 OSI 参考模型中,物理层是第一层,是整个开放系统的基础,向下直接与物理传输介质相连接。物理层协议是各种网络设备进行互联时必须遵守的底层协议,对数据链路层屏蔽了物理传输介质,实现了两个物理设备之间二进制比特流的透明传输。具体讲,物理层具有如下功能:

(1)为数据终端设备(Data Terminal Equipment,DTE)提供参考数据的通路。数据通路可以是一个物理介质,也可以是多个物理介质连接而成。一次完整的数据传输,包括激活物理连接、传送数据和终止物理连接。所谓激活,就是不管有多少物理介质参与,有要将通信的两个数据终端设备连接起来,形成一条通路。

(2)形成适合数据传输的实体,用来提供数据传送服务。物理层不但要保证数据的正确传送,而且要提供足够的带宽,以减少信道拥塞。传输数据的方式要满足点到点、点

到多点、串行或并行、半双工或全双工和同步或异步传输的需要。

(3)完成信道状态评估、能量检测、收发器管理、物理层属性管理等工作。

OSI 参考模型中物理层标准化工作要比数据链路层、网络层等高层慢。其原因有两点:一是与物理层设计的具体物理设备、传输介质与通信手段的复杂性有关;另一个更重要的原因是在 ISO 提出的 OSI 参考模型之前,许多属于物理层的模型和协议就已经提出,并在某些领域已形成相当的工业生产规模。这些模型、协议没有严格遵循分层的方法与原则,也没有像 OSI 那样分为服务定义与协议的规则说明。在现实情况下,要想把已有的物理层模型和协议统一到 OSI 物理层服务定义与协议说明的框架之下难度很大。关于物理层标准,目前已经提出了物理层服务定义的方案,但仍处于理论研究阶段。

1. 物理层的传输介质和互联设备

物理层的传输介质包括架空明线、平衡电缆、光纤和无线信道等。通信用的互联设备是指数据终端设备和数据电路终端设备(Data Circuit Terminal Equipment,DCE)间的连接设备,如各种插头、插座等。通常将具有一定数据处理能力和具有发送、接收数据能力的设备称为数据终端设备,又称为物理设备,如计算机、I/O 设备终端等;而把介于 DTE 与传输介质之间的设备称作 DCE,DCE 是数据通信设备或电路连接设备,如调制解调器等。DCE 在 DTE 与传输介质之间提供信号变换和编码功能,并负责建立、维护和释放物理连接。

在物理层通信过程中,DCE 一方面要将 DTE 传送的数据按比特流顺序发往传输介质,同时也要将传输介质接收到的比特流顺序传送给 DTE。因此在 DTE 与 DCE 之间,既有数据信息传输,也有控制信息传输。

2. 物理接口标准

物理层接口标准实际上是 DTE 与 DCE 或其他通信设备之间的一组约定,主要解决如何连接的问题。反映在物理接口标准中的物理层接口具有如下 4 个特性。

(1)机械特性。物理层的接卸特性规定了物理连接时所使用可接插连接器的形状和尺寸,连接器中引脚的数量与排列情况等。

(2)电气特性。物理层的电气特性规定了在物理连接上传输二进制比特流时,线路上信号电平高低、阻抗及阻抗匹配、传输速率与距离限制。

(3)功能特性。物理层的功能特性规定了物理接口上各条信号线的功能分配和确切定义。物理接口信号线一般分为数据线、控制线、定时线和地线。

(4)规程特性。物理层的规程特性定义了信号线进行二进制比特流传输线的一组操作过程,包括各信号线的工作规则和时序。

目前用于物理层的接口标准已有很多种,也比较成熟,其中使用比较广泛的物理接口标准有美国电子工业协会(EIA)的 RS-232-C 和 RS-447,以及国际电报电话咨询委员会 CCITT 系列和 X 系列,如 X.21 等。

7.2 物理层主要技术

无线通信物理层协议的主要技术包括介质选择、频段选择、调制技术以及扩频技术等。

7.2.1　通信介质及频段

无线通信的介质包括电磁波和声波。电磁波是最主要的无线通信介质，而声波一般仅用于水下无线通信。按照波长，电磁波可分为无线电波、微波、红外线、毫米波以及光波等。

无线电波很容易产生，可以传播很远，很容易穿过建筑物，因此被广泛用于室内或室外的无线通信。无线电波同时还是全方向传播的，即它能向任意方向传播，因此发射和接收装置不必在物理上很精确地对准。无线电波的传播特性与频率有关，在较低频率上，无线电波能轻易地通过障碍物，但是能量随着与信号源距离 r 的增大而急剧减小，大致为 $1/r^3$；在高频上，无线电波趋于直线传播并受障碍物的阻挡，还会被雨水吸收。在整个无线电频段上，无线电波易受发动机（发动机运转是将产生多次谐波的电磁噪声）和其他电子设备的干扰。另外，由于无线电波传播距离远，用户间的相互串扰也是个大问题。出于这个原因，每个国家和国际上都有关于频率使用的授权协议。

在 100MHz 以上，微波沿直线传播，因此可以集中于一点。通过类似电视接收器的抛物状天线，把所有的能量集中于一小束，便可以获得极高的信噪比，但是发射接收天线必须精确地对准。除此以外，这种方向性使成排的多个发射设备可以和多个接收设备通信而不会发生串扰。由于微波沿直线传播，所以如果微波塔相距太远，地表就会挡住去路，因此需要中继。和低频无线电波不一样，微波不能很好地穿过建筑物。

无导向的红外线和毫米波被广泛用于短距离通信。相对有方向性的无线电波，其收发设备容易制造，且价格便宜。红外线的主要缺点是不能穿透坚实的物体。从另一个角度说，红外线不能穿透坚固的墙壁也是优点，这意味着一间房屋里的红外系统不会对其他房间里的系统产生串扰，而且，正是由于这个原因，红外系统防窃听的安全性要比无线电系统好。基于这些原因，红外线的使用不受国家无线电管理委员会的限制。

光波及测光的装置可以用极低的成本提供极高的带宽，同时它还很容易安装。和微波不一样，使用光波不需要联邦通讯委员会（Federal Communications Commission，FCC）授权。光波的缺点之一是不能穿透雨或浓雾。与无线电传输相比，光波传输不需要复杂的调制、解调机制，接收器电路简单，单位数据传输功耗较小。

7.2.2　调制与解调技术

调制与解调技术是无线通信系统的关键技术之一。一般来说，信号源的编码信息（信源）含有直流分量和频率较低的频率分量，称为基带信号。基带信号往往不能作为传输信号，因此必须把基带信号转变为相对基带频率而言频率非常高的带通信号以适合于信道传输。这个带通信号称为已调信号，而基带信号称为调制信号。调制是通过改变高频载波的幅度、相位或者频率，使其随着基带信号幅度的变化而变化来实现的。解调则是将基带信号从载波中提取出来，以便预定的接收者（信宿）处理和理解的过程。

调制是通信系统中非常重要的技术，具有如下作用[3]：

（1）信号与信道匹配。自然界中要传送的信号大多数为低通型信号，然而，信道大多为带通型，为使低通型信号在带通型信道中传输，这就需要调制。因此调制的本质就是把信号的频谱搬移到信道的带通频带之内，使信号频谱与信道特性匹配。

(2)电波有效辐射。根据无线电波传播原理,为了有效地把电磁能量耦合到空间,天线直径或长度至少与传输信号波长相当。因此,为了有效辐射必须进行调制。

(3)频率分配。随着通信、广播、电视等的发展,空间频率资源越来越紧张,为了利用频率资源,需对频率进行分配,使通信、广播、电视等互不干扰。要使通信、广播、电视指定的频段工作,必须依靠调制来实现。

(4)减小干扰。因为干扰信号的时间、频谱位置是不断变化的,可以通过调制减小干扰的影响,实现通信;另外,调制还可以将信号安排在人们特意设计的频段中,使滤波、放大等变得容易实现。

综上所述,调制对通信系统的有效性和可靠性有很大影响,采用何种方法调制和解调往往在很大程度上决定着通信系统的质量。

根据调制中采用的基带信号的类型,又可以将调制分为模拟调制和数字调制。模拟调制就是用模拟基带信号对高频载波的某一参量进行控制,使高频载波随着模拟基带信号的变化而变化。数字调制则是用数字基带信号对高频载波的某一参量进行控制,使高频载波随着数字基带信号的变化而变化。正弦载波有振幅、频率和相位3个参量,根据原始信号所控制参量的不同,调制分为幅度调制(Amplitude Modulation,AM)、频率调制(Frequency Modulation,FM)和相位调制(Phase Modulation,PM)。如今,通信系统都在由模拟制式向数字制式过渡,因此数字调制技术成为了主流的调制技术。另外,数字调制信号为二进制矩形全占空脉冲序列时,由于该序列只有“有电”和“无电”两种状态,它能用电键控制,故称为键控信号,因此上述数字的调幅、调频、调相又可以分别称为幅移键控(Amplitude Shift Keying,ASK)、频移键控(Frequency Shift Keying,FSK)和相移键控(Phase Shift Keying,PSK),其波形图和发生电路的简图如图7.1所示。

无线通信信道具有带宽有限、干扰和噪声影响大以及存在多径衰落等基本特征。因此,在选择无线调制方式时,必须考虑采取抗干扰能力强的调制方式,能适用于衰落较快的信道,占有较小的带宽以提高频谱利用率,并且带外辐射要小,以减小对邻近频道的干扰。然而简单的ASK、PSK和FSK因传输效率低而无法满足移动通信的要求。为此,需要专门研究一些抗干扰能力强、误码性能好、频谱利用率高的调制方式,尽可能地提高单位频率内传输数据的比特率,以适用于无线通信的窄带数据传输的要求。

20世纪80年代以来,人们十分重视调制技术在无线通信系统中的应用,以寻求频谱利用率更高、频谱特性更好的数字调制方式。由于振幅键控信号的抗噪声性能不够理想,因此,目前在无线通信中广泛应用的调制技术主要有频移键控和相移键控两大类[4,5]。

1. 频移键控

FSK在无线短波通信中应用广泛,这是因为它除了设备简单、调制与解调方便外,更重要的是这种调制方式具有较好的抗多径时延性能。目前,广泛应用的频率键控方法主要有最小频移键控(Minimum Shift Keying,MSK)和高斯滤波最小频移键控(Gaussian filtered Minimum Shift Keying,GMSK)[6]。

MSK是FSK的一种改进形式。在FSK方式中,每一码元的频率不变或者跳变一个固定值,而两个相邻的频率跳变码元信号,其相位通常是不连续的。所谓MSK方式,就是FSK信号的相位始终保持连续变化的一种特殊方式。MSK信号以其恒包络、连续相位、带外辐射小,便于在非线性信道中传输等优点得到广泛应用。

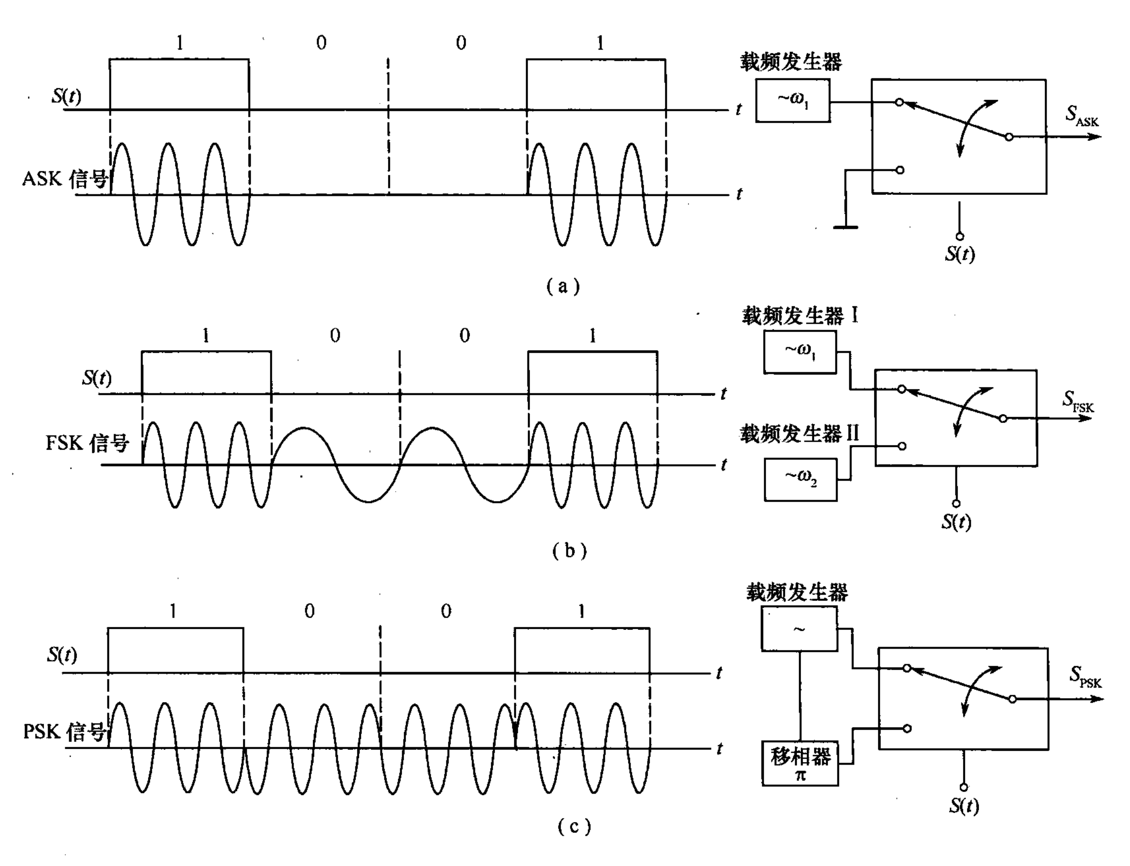


图 7.1　三种数字调制的波形图与产生简图

(a)幅度调制；(b)频率调制；(c)相位调制。

二进制最小频移键控信号可表示为

$$S(t) = \cos[\omega_c t + \omega_d \alpha_k t + \varphi_k],\quad kT_b \leqslant t \leqslant (k+1)T_b \tag{7.1}$$

式中：ω_c 为载频；ω_d 为频偏；$\alpha_k = \pm 1$ 为传输的数据；T_b 为码元宽度；φ_k 为第 k 个码元中的相位常数，为 0 和 π 的整数倍，它在时间 $kT_b \leqslant t \leqslant (k+1)T_b$ 的条件下保持不变。

根据在一个码元期间内，其相位差应该严格地等于 π，则有

$$(\omega_c + \omega_d)T_b - (\omega_c - \omega_d)T_b = \pi \tag{7.2}$$

由此可得

$$\omega_d = \frac{\pi}{2T_b}\left(\text{或} f_d = \frac{1}{4T_b}\right) \tag{7.3}$$

将式(7.3)代入式(7.1)，MSK 信号可表示为

$$S(t) = \cos[\omega_c t + \frac{\pi}{2T_b}\alpha_k t + \varphi_k] \tag{7.4}$$

信号的附加相位为

$$\theta(t) = \frac{\pi\alpha_k}{2T_b}t + \varphi_k \tag{7.5}$$

展开 $S(t)$ 为

$$S(t) = \cos\theta_k \cos\omega_c t - \sin\theta_k \sin\omega_c t \tag{7.6}$$

由于 $\varphi_k = 0$ 或 π，则 $\sin\varphi_k = 0$，故有

$$\begin{cases} \cos\theta(t) = \cos\left(\dfrac{\pi t}{2T_b}\right)\cos\varphi_k \\ \sin\theta(t) = -\alpha_k \sin\left(\dfrac{\pi t}{2T_b}\right)\cos\varphi_k \end{cases} \tag{7.7}$$

将式(7.7)代入式(7.6)，可得

$$S(t) = \cos\varphi_k \cos\left(\frac{\pi t}{2T_b}\right)\cos\omega_c t - \alpha_k \cos\varphi_k \sin\left(\frac{\pi t}{2T_b}\right)\sin\omega_c t =$$

$$I_k \cos\left(\frac{\pi t}{2T_b}\right)\cos\omega_c t + Q_k \sin\left(\frac{\pi t}{2T_b}\right)\sin\omega_c t \tag{7.8}$$

式中：$I_k = \cos\varphi_k$；$Q_k = -\alpha_k \cos\varphi_k$；$kT_b \leqslant t \leqslant (k+1)T_b$；$I_k$ 为同相分量；Q_k 为正交分量；$\cos\left(\frac{\pi t}{2T_b}\right)$为同向加权函数；$\sin\left(\frac{\pi t}{2T_b}\right)$为正交分量的加权函数。

GMSK 在 MSK 高斯低通滤波器之前加入一个基带信号预处理滤波器，即高斯低通滤波器，由于其将基带信号变换成高斯脉冲信号，包括无陡峭边沿和拐点，从而达到改善 MSK 信号频谱特性的目的。

实现 GMSK 信号的调制，关键是设计一个性能良好的高斯低通滤波器，它必须具有如下特性：

(1)有良好的窄带和尖锐的截止特性，以滤除基带信号中多余的高频部分。

(2)脉冲响应过冲量应尽量小，防止已调瞬时频偏过大。

(3)输出脉冲响应曲线的面积对应的相位为 $\pi/2$，是调制系数为 1/2。

满足这些特性的高斯低通滤波器，其频率传输函数为

$$H(f) = \exp(-\alpha^2 f^2) \tag{7.9}$$

式中：α 为与滤波器 3dB 带宽 B_b 有关的一个待定常数，选择不同的 α，滤波器的特性随之而变。

通常令高斯低通滤波器的传输函数值为$\frac{1}{\sqrt{2}}$时，定义滤波器的 3dB 带宽，即

$$B_b = \frac{\sqrt{\ln 2}}{\sqrt{2} \cdot \alpha} = 0.5887/\alpha \tag{7.10}$$

由式(7.10)可知，改变 α 时，带宽 B_b 也随之而变。

2. 相移键控

目前，主流的相移键控包括二相相移键控(Binary reference Phase Shift Keying, BPSK)、四相相移键控(Quadrature reference Phase Shift Keying, QPSK)、正交四相相移键控(Orthogonal Quadrature reference Phase Shift Keying, OQPSK)和 $\pi/4$ 正交相移键控($\pi/4$ Quadrature reference Phase Shift Keying, $\pi/4-$QPSK)。

BPSK 是采用载波(0,π)两种相位传送二进制数字(1,0)的相移调制方式。BPSK 信号的数学表达式为

$$S(t) = \cos(\omega_c t + \theta_k) \tag{7.11}$$

式中:θ_k 为 $kT \leqslant t \leqslant (k+1)T$ 时间的附加相位。当基带信号为 1 时,θ_k 为 0,当基带信号为 0 时,θ_k 为 π。

显然,BPSK 信号可以看成是双极性基带信号乘以载波信号而产生的,即

$$S(t) = s'(t)\cos(\omega_c t) \tag{7.12}$$

式中:$s'(t)$为双极性数字基带信号。

为了提高信道的俄频谱利用率,人们在 BPSK 的基础上开发出 QPSK,其信息传播速率是 BPSK 的 2 倍。QPSK 是一种四进制的相应键控调制方式,可以看成是两正交的二相调制合成,即码元的 4 种组合(00,01,10,11)对应于正弦载波的 4 个相位(0, ±π/2,π)或(±π/4, ±3π/4)。

调制信号可表示为

$$S(t) = \cos(\omega_c t + \theta_k) \tag{7.13}$$

式中:θ_k 为 $kT \leqslant t \leqslant (k+1)T$ 时间的附加相位,θ_k 可以是 0、±π/2、π 或 ±π/4、±3π/4,对应情况如图 7.2 所示,QPSK 相位真值如表 7.1 所示。

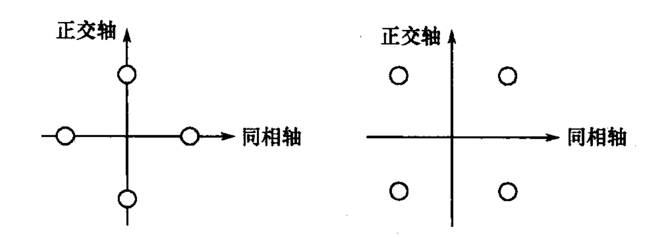


图 7.2　QPSK 相位的两种情况

式(7.13)也可以写成

$$S(t) = \cos\omega_c t\cos\theta_k - \sin\omega_c t\sin\theta_k \tag{7.14}$$

表 7.1　QPSK 相位真值表

	二进制码元		QPSK 相位		二进制码元		QPSK 相位
	A	B			A	B	
方案 1	1	1	45°	方案 2	1	1	0°
	0	1	135°		0	1	70°
	0	0	225°		0	0	180°
	1	0	315°		1	0	270°

为了改善 QPSK 信号的频谱特性,出现了改进型的交错正交四相相移键控 OQPSK。OQPSK 克服了 QPSK 信号在码元转换时刻存在相位突变 180°的问题,改善了信号经非线性信道时的频谱扩散[7]。

OQPSK 是继 QPSK 之后发展起来的一种恒包络数字调制技术。与普通的 QPSK 相比,OQPSK 的同相数据流 I 与正交数据流 Q 在时间上相互错开了一个码元间增量 T_b,如

图 7.3 所示。即半个符号周期 $T_s = 2T_b$，与 QPSK 不同，OQPSK 信号中的 I、Q 数据流每次只有一个可能发生极性转换。

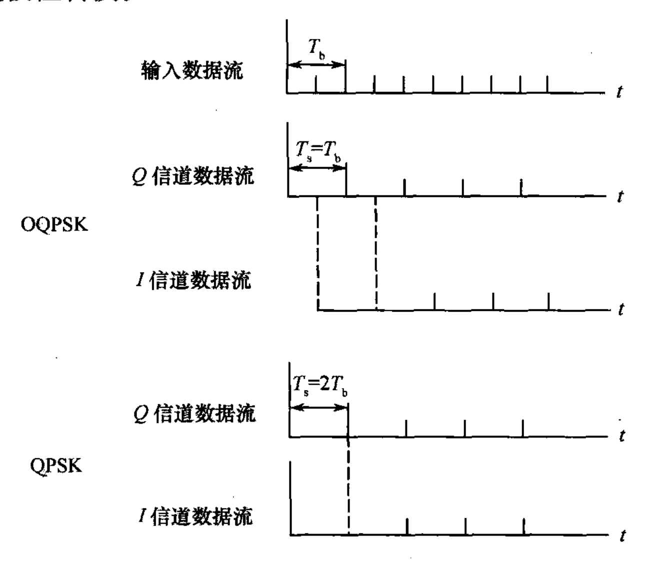


图 7.3　OQPSK 和 QPSK 数据流的时间关系

因此，如表 7.2 所列，当新的输入比特进入调制器的 I 或 Q 信道时，输出的 OQPSK 信号只有 0°、±70°三个相位跳变值，不可能出现 180°相位跳变。所以，OQPSK 的信号包络起伏比 QPSK 的信号小，经限幅放大后频带展宽得少，减少了随机相位的影响，降低了对射频放大器的线性要求，故 OQPSK 性能优于 QPSK。

表 7.2　OQPSK 调制的相位图

数据序列 $I_{t0}\ Q_{t1}\ I_{t2}$	OQPSK 信号在 t_2 的相位变化	合成矢量	数据序列 $I_{t0}\ Q_{t1}\ I_{t2}$	OQPSK 信号在 t_2 的相位变化	合成矢量
000	初始 0°	Q	101	初始 0°	Q
001	+90°	Q	100	-90°	Q
010	-90°	Q	110	+90°	Q
010	0°	Q	111	0°	Q

π/4 - QPSR 是在 QPSK 和 OQPSK 信号的基础上发展起来的调制技术，进一步提高了频谱特性，有利于采用差分检测。

设 π/4 - QPSK 的已调信号为

$$S(t) = \cos(\omega_c t + \theta_k) \tag{7.15}$$

式中：θ_k 为 $kT \leqslant t \leqslant (k+1)T$ 时间的附加相位。

将式(7.15)展开，得

$$S(t) = \cos\omega_c t\cos\theta_k - \sin\omega_c t\sin\theta_k \tag{7.16}$$

θ_k 是前一码元附加相位 θ_{k-1} 与当前码元相位跳变量 $\Delta\theta_k$ 之和，表示了当前码元的附加相位，即

$$\theta_k = \theta_{k-1} + \Delta\theta_k \tag{7.17}$$

设 I 通道的幅值为

$$V_I(t) = \cos\theta_k = \cos(\theta_{k-1} + \Delta\theta_k) = \cos\theta_{k-1}\cos\Delta\theta_k - \sin\theta_{k-1}\sin\Delta\theta_k \tag{7.18}$$

设 Q 通道的幅值为

$$V_Q(t) = \sin\theta_k = \sin(\theta_{k-1} + \Delta\theta_k) = \sin\theta_{k-1}\cos\Delta\theta_k + \cos\theta_{k-1}\sin\Delta\theta_k \tag{7.19}$$

令

$$V_{Q_m} = \sin\theta_{k-1}, V_{I_m} = \cos\theta_{k-1}$$

则 I、Q 通道的幅值分别为

$$V_I(t) = V_{I_m}\cos\Delta\theta_k - V_{Q_m}\sin\Delta\theta_k \tag{7.20}$$

$$V_Q(t) = V_{Q_m}\cos\Delta\theta_k + V_{I_m}\sin\Delta\theta_k \tag{7.21}$$

式(7.21)表明前一码元的两正交信号幅度与当前码元的两正交信号幅度之间的关系取决于当前码元的相位跳变量。而当前码元的相位跳变量，又取决于信号变换电路的输入码组。表7.3给出了双比特信息 I_k、Q_k 和相邻码元间相位跳变 $\Delta\theta_k$ 之间的对应关系。

表7.3 I_k，θ_k 与 $\Delta\theta_k$ 的对应关系

I_k	Q_k	$\Delta\theta_k$	$\cos\Delta\theta_k$	$\sin\Delta\theta_k$
1	1	$\pi/4$	$1/\sqrt{2}$	$1/\sqrt{2}$
-1	1	$3\pi/4$	$-1/\sqrt{2}$	$1/\sqrt{2}$
-1	-1	$-3\pi/4$	$-1/\sqrt{2}$	$-1/\sqrt{2}$
1	-1	$-\pi/4$	$1/\sqrt{2}$	$-1/\sqrt{2}$

由表7.3可见，码元转换时刻的相位不可能产生 $\pm\pi$ 的相位跳变，信号的频谱特性得到较大的改善，同时也可以看到 V_Q 和 V_I 只可能有 $0, \pm\frac{1}{\sqrt{2}}, \pm 1$ 五种取值。

7.2.3 扩频技术

扩频又称扩展频谱，是指发送端将待发送的数据用扩频调制实现频谱扩展，再进行传输，接收端采用同样的扩频码进行相关处理及解调，恢复原是数据信号的通信方式。显然，这种通信方式与常见的窄带通信方式不同，它是扩展频谱后进行宽带通信，再经相关处理恢复成窄带信号解调出数据。扩频采用高速编码技术，扩展传输信息的频带宽度，使传输信息的带宽远大于信息本身所占的带宽，例如，信息本身的带宽为 Δf，传输信息的带

宽为 ΔF，则 $\Delta F > \Delta f$。在接收端使用相关解调技术进行解扩，恢复所传输的原始信息。

上述扩频通信的定义包含 3 个方面的意思：第一，信号的频谱被扩展了。例如，语音所占的带宽为 300Hz ~ 3400Hz，对于一般的调频通信，调制带宽比信息带宽只大几倍到十几倍，而扩频通信调制传输带宽比信息带宽大几百倍到几千倍。第二，采用高速编码技术，即采用扩频码序列调制方式来展宽频谱。例如，窄脉冲的频谱很宽，1ms 宽度的脉冲其带宽约为 1MHz，因此，扩频通信就是采用高速的编码序列来调制，使频谱展宽。第三，接收端采用相关解调技术进行解扩。

扩频通信的理论基础是通信理论中具有重要意义的香农公式，即

$$C = B_b(1 + S/N) = B_b(1 + S/n_0B) \tag{7.22}$$

式中：C 为信道容量，即信道传输速率的最大值；B_b 为传输信道带宽；S 为信号平均功率；N 为噪声平均功率；n_0 为噪声功率谱密度。

由香农公式看出：可以通过带宽和信噪比的互换达到信道容量保持不变的目的。因此，采取减少发射功率，增加带宽的方法可以保持通信容量不变。B_b 和 S 的互换是通过改变信号波形实现的，即采用高速编码技术，这就是扩频技术的理论基础。扩大传输带宽可以增大信道容量，但是扩大传输频带宽度不可能使信道容量无限地增大。

扩频通信与一般的无线电通信系统相比，主要是在发射端增加了扩频调制，在接收端增加了扩频解调的过程。在发射端，利用一组速率元高于信号速率的伪随机噪声码（Pseudo Noise code，PN）对原信号码进行扩频调制，一般是将信号展宽到几兆的频带上，然后将扩频后的信息调制到空间传输的载频上进行发送，通常发射的载频是千兆数量级；在接收端经解调后，利用相同的 PN 码进行解扩，把展开的信号能量从宽带上收拢回来，凡与 PN 码相关的带宽信号经解调还原为原来的窄带信号，而其他与 PN 码不相关的带宽噪声仍维持宽带，解调后的窄带信号再经窄带滤波后，分离出有用信号，这样使信噪比得以极大地提高，误码率大大降低。

由此可见，扩频通信具有扩频码调制和信号相关处理两大特点。正是这两大特点，使扩频通信方式具有许多突出优点，主要有以下几个方面：

（1）很强的抗干扰能力。由于将信号扩展到很宽的频带上，在接收端对扩频信号进行相关处理，即带宽压缩，恢复成窄带信号。对干扰信号而言，由于与扩频用的 PN 码不相关，被扩展到很宽的频带上，使之进入信号通频带内的干扰功率大大降低，相应地增加了信噪比，因此具有很强的抗干扰能力。其抗干扰能力与频带的扩展倍数成正比，频谱扩展得越宽，抗干扰的能力越强。

（2）可进行多址通信。扩展频谱通信本身就是一种多址通信方式，称为扩频多址（Spread Spectrum Multiple Access，SSMA），实际上是 CDMA 的一种，用不同的扩频码组成不同的网。虽然扩展频谱系统占用了很宽的频带，但由于各网在同一时刻共用一频段，其频段利用率甚至比单路单载波系统还要高。

（3）安全保密。由于扩频系统将传送的信息扩展到很宽的频带上去，其功率密度随频谱的展宽而降低，甚至可以将通信信号淹没在噪声中。因此，其保密性很强，要截获、窃听或侦察这样的信号是非常困难的，除非采用与发送端相同的扩频码且与之同步后进行相关的检测，否则对扩频信号是无能为力的。由于扩频信号功率谱密度很低，在美、日、欧

洲等许多国家对专用频段,如工业、科学和医疗频段,只要功率谱密度满足一定的要求,就可以不经批准使用该频段。

(4)抗多径干扰。在无线通信、室内通信等通信环境下,多径干扰是非常严重的,系统必须具有很强的抗干扰能力,才能保证通信的畅通。扩展频谱技术具有很强的抗多径能力,它是利用扩频所用的扩频码的相关特性来达到抗多径干扰,甚至可以利用多径能量来提高系统的性能。

扩频技术按其工作方式可分为以下几种:直接序列扩频(Direct Sequence Spread Spectrum,DSSS)、跳频(Frequency Hopping Spread Spectrum,FHSS)、跳时(Time Hopping Spread Spectrum,THSS)、以及线性调频(chirp Spread Spectrum,chirp - SS)等方式[8~11]。

1. 直接序列扩频

直接序列扩频是直接利用具有高码率的 PN 码,采用各种调制方式在发射端扩展信号的频谱;在接收端用相同的 PN 码进行解码,将展宽的扩频信号还原成原始信息。具体地说,就是将信源于一定的 PN 码进行模二加。例如,在发射端,将“1”用 11000100110,而将“0”用 00110010110 表示,这个过程就实现了扩频;而在接收端,只要将收到的序列 11000100110 恢复成“1”,将 00110010110 恢复成“0”,就完成了解扩。这样信源速率就提高了 11 倍,同时使处理增益达到 10dB 以上,从而有效提高整机信噪比。

图 7.4 给出直接序列扩频系统的原理框图。

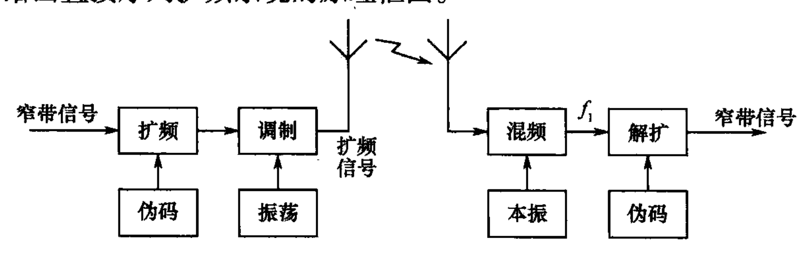


图 7.4 直接扩频系统原理图

基带信号的信号码是欲传输的信号,通过扩频将其频谱展宽,频谱展宽后的序列多采用 PSK 调制进行射频调制,其输出则是扩展频谱的射频信号,经天线发射出去。在接收端,射频信号经混频后变为中频信号,它用与发射端相同的编码序列反扩展,将宽带信号解扩,解扩后的中窄带信号经普通通信信息解调器进行解调,恢复成原始的信号码。

由频谱扩展对抗干扰性带来的好处,称为扩频增益,表示为

$$G_p = B_w / B_s \tag{7.23}$$

式中:B_w 为发射扩频信号的带宽,与所采用的 PN 码速率有关;B_s 为信码的速率。

为获得高的扩频增益,通常希望增加射频带宽。

2. 跳频

跳频扩频是将数字信息与 PN 码相加后,离散地控制射频载波振荡器的输出频率,使发射信号的频率随 PN 码的变化而跳变,发射频率的次序决定于该编码序列。跳频系统中的载频受 PN 码的控制,不断地随机跳变。接收端只有知道跳频图,才能正确接收。通常接触到的无线通信系统都是载波频率固定的通信系统,如移动电话等,所以也称为定频通信。这种定频通信系统,一旦受到干扰,就将使通信质量下降,严重时甚至使通信中断;

另外在敌我双方的通信对抗中，敌方总是企图发现我方的通信频率，以便截获所传送的信息内容，或者发现我方通信机所在的方位，定频通信系统容易暴露目标 且易于被截获。而采用跳频通信就比较隐蔽也难以被截获。

因此，跳频通信具有抗干扰性、抗截获的能力，并能做到频谱资源共享。所以在现代化的电子战中，跳频通信已显示出巨大的优越性；跳频通信也应用到民用通信中以抗衰落、抗多径、抗网间干扰和提高频谱利用率。图 7.5 给出了跳频系统的原理方框图。

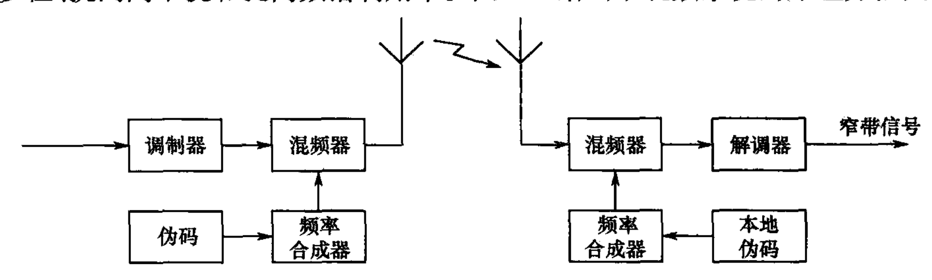


图 7.5　跳频系统原理图

如果图 7.6 中的频率合成器被设定在某一频率上，这就是普通的数字调制系统，其射频为一窄带频谱。当利用 PN 码随机设定频率合成器时，发射机的振荡频率在很宽的频率范围内不断地改变，从而使射频载波在很宽的范围内变化，于是形成宽带离散谱。接收端必须以同样的 PN 码设定本地频率合成器，使其与发射端的频率作相同的改变，即收发跳频必须同步，这样才能保证通信的建立。解决同步及定时是实现调频系统的关键问题。

跳频系统处理增益的定义为

$$G_p = B_w/B_s = N \tag{7.24}$$

式中：B_w 为系统带宽；B_s 为单载频率带宽；N 为可供选用的频率数目。

3. 跳时

跳时扩频用 PN 码控制信号发送时刻及信号持续时间的长短。跳时是使发射信号在时间轴上跳变，先把时间轴分成许多时片，哪个时片发射信号由扩频码序列进行控制，发射信号的“有”、“无”同 PN 码一样是伪随机的。可以将跳时理解为用一定码序列进行选择的多时片的时移键控。由于信号在时域被压缩，或者说由于采用窄得很多的时片去发送信号，相对而言，信号的频谱也就展宽了。在发射端，输入的数据先存储起来，由扩频码发生器的扩频码序列去控制通/断开关，经二相或四相调制后，再经射频调制后发射；在接收端，由射频接收机输出的扩频信号，经本地产生的与发射端相同的扩频码序列去控制通/断开关，再经二相或四相解调器，送到数据存储器和再定时后输出数据。只要收、发两端在时间上严格同步进行，就能正确地恢复原始数据。跳时也可看成是一种时分系统，不同之处在于它不是在一帧中固定分配一定位置的时片，而是由扩频码序列控制的按一定规律跳变位置的时片。跳时系统的处理增益等于一帧中所分的时片数。由于简单的跳时抗干扰性不强，很少单独使用，跳时一般和跳频结合起来使用，两者一起构成一种时频跳变系统。

跳时技术是超宽带通信技术的重要组成部分，在超宽带通信系统中起着至关重要的作用。跳时序列是超宽带实现多址通信的来源，跳时序列的数目直接决定了超宽带通信系统的用户数目，同时它也是同步和信道检测的可靠保证，所以跳时序列性能的优劣对整

个超宽带通信系统性能有直接影响。为了满足系统的要求，跳时序列必须具有良好的相关注，即良好的自相关性和互相关性。

4. 线性调频

在脉冲线性扩频系统中，射频脉冲信号的载频在信息脉冲持续时间内作线性变化，其瞬时频率随时间变化，即信号载频从原来单一频率得到了扩展，系统获得处理增益。因其频率在较宽的频带内变化，信号的带宽被展宽了。由于这种线性调频信号占用的频带宽度远大于信息带宽，所以也是一种扩频调制技术。它利用一系列短促的、可同步的扫描频率 Chirps 作为载体，每个线性调频波一般持续 100μs，它代表最基本的通信符号时间（Unit Symbol Time, UST），这些 Chirps 覆盖了 100kHz ~ 400kHz 的频带，并总是以 200kHz ~ 400kHz 的频率开始，继而以 100kHz ~ 200kHz 的频率结束。由于 Chirps 信号的线性扫描带宽比信号带宽要大得多，其线性加速度较高，而连续波干扰（Continuous Wave Jamming）的频率加速度一般是稳定的，所以将滤波器设计成只能通过具有特定角加速度的信号，就可以将连续波干扰排除在外。另外，这种线性调频波形还具有很强的自相关性，这种模糊逻辑的相关性决定所有连接在网络上的设备可以同时识别从网上任意设备发出的这种独特波形，并且不需要在发送和接收设备间进行同步。

线性调频信号的表达形式为

$$S_i(t) = \mathrm{rect}(t/T)\cos(2\pi f_0 t \pm 1/2\mu t^2) \tag{7.25}$$

式(7.25)中矩形调制函数为

$$\mathrm{rect}(t/T) = \begin{cases} 1 & (|t/T| \leqslant 1/2) \\ 0 & (|t/T| > 1/2) \end{cases} \tag{7.26}$$

式(7.25)和式(7.26)中，f_0 为线性调频信号的中心频率；T 为线性调频信号的时间宽度，$T = 1/f_b$，f_b 为传输信息速率；μ 为线性调频信号的变频速率因子，$\mu = 2\pi B/T$；B 为线性调频信号的瞬时带宽，$B = f_{max} - f_{min}$。

在 T 这段时间内，线性调频信号的载波频率按线性规律变化，其瞬时频率可写成：

$$f_i = \frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}t}\left[\omega_0 t + \frac{1}{2}\mu t^2\right] = f_0 + \mu t/2\pi, \qquad \left(t \in \left[-\frac{T}{2}, \frac{T}{2}\right]\right) \tag{7.27}$$

线性调频信号的频谱特性可以根据傅里叶变换公式由数学方法求出，或在计算机上直接用快速傅里叶变换（FFT）得出。

7.3 无线传感器网络物理层协议研究现状

物理层协议涉及无线传感器网络采用的传输介质、选择的频段以及调制方式。此外，为了实现低能耗目标，目前对无线传感器网络物理层的研究提出了一些节能机制[12,13]。

7.3.1 介质和频段选择研究

目前，无线传感器网络采用的传输介质主要包括无线电、红外线和光波等。无线电波在通信方面没有特殊的限制，比较适合无线传感器网络在未知环境中的自主通信需求，是目前无线传感器网络的主流传输方式。在无线电频率选择方面，除军事应用外一般选用

ISM 频段。选用 ISM 频段的主要优点是 ISM 频段是无需注册的公用频段,具有大范围的可选频段,没有特定的标准,可以灵活使用。面对传感器节点小型化、低成本、低功耗的特点,人们提出在欧洲使用 433MHz ISM 频段,在美国使用 715MHz ISM 频段。P. Favre 等人采用硅 IC 技术完成了美国使用的 715MHz ISM 频段的无线接收器的设计,旨在实现低成本、低能耗。T. Melly 等人[14]1999 年采用标准数字 CMOS 处理技术实现了 433MHz ISM 频段的无线收发器设计。其中,重点设计了无线收发器的两个关键模块:

(1)功率放大器由两个完全集成的 A 类预放大器和一个微分 C 类输出放大器组成。

(2)一个压缩的、低电压、低功率的完全集成的 LNA(Low Noise Amplifier)混频器。

此外,DARPA 资助 WINS 项目也研究了如何采用 CMOS 电路技术实现硬件的低成本制作。

红外线作为无线传感器网络的可选传输方式,其最大的优点在于其传输方式不受无线电干扰,且红外线的使用不受国家无线电管理委员会的限制。然而,红外线对非透明物体的透过性极差,只能在一些特殊的无线传感器网络应用中使用。

光波传输与无线电传输相比,不需要复杂的调制解调机制,接收器的电路简单,单位数据传输功率小。在 Smart Dust 项目中,研究人员开发了基于光波传输,具有传感、计算能力的自治系统;提出了两种光波传输机制,即使用三面直角反光镜(CCR)的被动传输方式和使用激光二极管、易控镜的主动传输方式。在被动传输方式中,传感器节点不需要安装光源,通过配置 CCR 来完成通信;在主动传输方式中,传感器节点使用激光二极管和主控激光通信系统来发送数据。光波与红外线相似,通信双方不能被非透明物体阻挡,因此只能在一些特殊的无线传感器网络应用中使用。

7.3.2 休眠机制

UC Berkeley 研发的 PicoRadio[17]项目采用无线电唤醒装置,该装置支持睡眠模式,由包含目的节点 ID 的唤醒信标唤醒目的节点,并通知其切换到相应的信道,从而实现在全负载周期运行时的能耗小于 100μW。

MIT 研发的 μAMPS 项目定义了节点的 5 种工作模式,即活动、准备、监听、观察(Observe)和深度睡眠。5 种工作模式下的 CPU、传感器、A/D 转换器和无线收发器的状态如表 7.4 所列。

表 7.4　节点工作模式

模 式	CPU 状态	传感器,A/D 转换器状态	无线收发器状态
活动	空闲	感知	发送/接收
准备	空闲	感知	接收
监听	睡眠	感知	接收
观察	睡眠	感知	关闭
深度睡眠	睡眠	关闭	关闭

μAMPS 结合无线传感器网络低负载周期的特点,通过切换工作模式实现了节能的目的。另外,在设计物理层时,μAMPS 指出,收发机在从睡眠模式到工作模式的转换能量可

能大于工作时消耗能量的情况，如图 7.6 所示。

节点 k 在 t_1 时刻完成了事件的处理，能耗为 P_0，下一个事件发生在 t_2 时刻，$t_2 = t_1 + t_i$，于是节点 k 决定转换到睡眠状态 S_k，睡眠状态的能耗为 P_k，设从活动状态转换到 S_k 的时间为 $\tau_{d,k}$，从 S_k 到活动态的转换时间为 $\tau_{u,k}$，那么状态转换节约的能量为

$$E_{s,k} = P_0 t_i - \left[\frac{P_0 + P_k}{2}\right](\tau_{d,k} + \tau_{u,k}) - P_k(t_i - \tau_{d,k}) \tag{7.28}$$

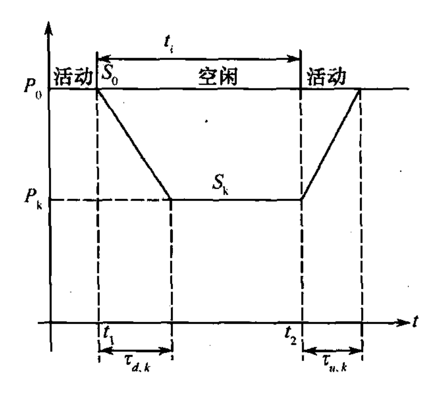


图 7.6　状态切换与能耗曲线

显而易见，并不是所有条件下的切换都可以实现节能。为了使 $E_{s,k} > 0$，得到 t_i 的阈值为

$$T_{th,k} = \frac{1}{2}\left[\tau_{d,k} + \left(\frac{P_0 + P_k}{P_0 - P_k}\right)\tau_{u,k}\right] \tag{7.29}$$

由式(7.28)和式(7.29)可知，转换时间越长，越节能。

另外，C. F. Chiasserini 与 R. R. Rao[16] 认为脉冲放电电池适合无线传感器网络的低负载周期、数据通信具有突发性等特征，因此可采用充电恢复效应来延长该电池的寿命。数据包传输持续时间的合理值为 1ms，因此，将时间维度离散化为 1ms 的间隔。假设数据源满足 Bernoulli 随机过程，即每个间隔产生数据包的概率为 P，那么电池的恢复概率为 $1 - P$；如果假设数据包产生后立刻传输，则电池需要产生 1ms 的脉冲用于数据发送，当电池的能量下降到阈值以下时放电终止。仿真结果表明了该方法可以提高电池效率。另外，采用放电整型技术，通过以延迟数据包的发送为代价，进一步提高电池效率。

7.3.3　调制和扩频机制

在调制和扩频机制选择方面，传统的无线通信系统需要考虑的重要指标有频谱效率、误码率、环境适应性，以及实现的难度和成本。无线传感器网络需要以节能和节约成本为主要指标的调制和扩频机制。

7.3.3.1　*M*-ary 调制机制

M-ary 调制机制，即多进制调制机制，采用高频载波的多种振幅。频率或相位表示数字信息。图 7.7 为四电平振幅调制的波形示意图，高频载波振幅有 0、A、2A、3A 四种，分别代表数字信息 0、1、2、3 或者双比特二进制输入信息 00、01、10、11。为了同时满足无线传感器网络最小化符号率和最大化数据传输率的指标，人们将 *M*-ary 调制机制应用于无线传感器网络。

二进制和 *M*-ary 调制机制比较：

(1)在码元速率相同的条件下，*M*-ary 调制的信息速率是二进制调制的 $\log_2 M$ 倍，因此，与二进制调制相比，*M*-ary 调制机制通过单个符号发送多位数据的方法减少了发射的时间，降低了发射功耗。

(2)对比二进制调制电路，首先在 *M*-ary 调制电路发信输入端应该增加 2 - *M* 电平变

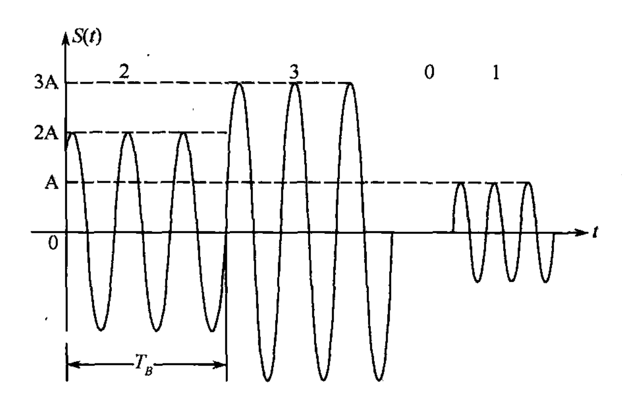


图 7.7　*M*-ary 振幅调制波形

换，相应在接收端应有 *M*-2 电平转换，另外该电路的取样判决有多个判决电平，如上述四电平调制，判决电平为 0.5A、1.5A、2.5A 三种，导致其取样判决电路比较复杂，如图 7.8 所示。

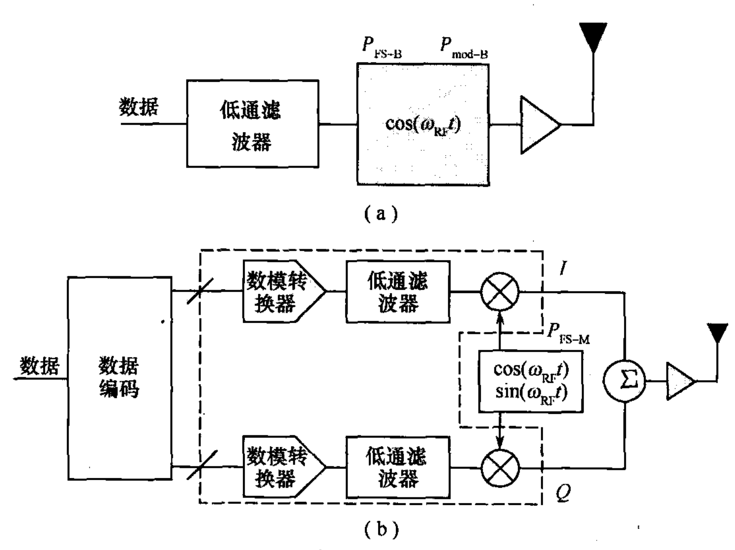


图 7.8　二进制和 *M*-ary 调制

(a)二进制调制；(b)*M*-ary 调制。

(3)如果以无线收发器的启动时间为主要条件，则二进制调制机制在启动时间较长的系统中更加节能、有效，而 *M*-ary 调制机制适用于启动时间较短的系统。

(4)当码元速率相同时，*M*-ary 调制带宽与二进制调制相同。

(5)*M*-ary 调制的误码率通常远大于二进制调制的误码率，当功率受限时，*M* 越大，误码增加越严重。

(6)*M*-ary 调制不能充分利用发射机功率。

综上所述，*M*-ary 调制虽然是一种高效的调制方式，但抗干扰能力较差。

7.3.3.2　差分编码相移调制

虽然 *M*-ary 可以通过最小化符号率和最大化数据传输率实现节能，但是简单的多相

位 M-ary 信号将降低功率放大器的效率，降低检测的敏感度，为了保持和恢复连接，则需要增加发射功率，从而导致额外的能量浪费。为了避免该问题，E. H. Callaway 等人[1]提出了准正交的差分编码相移调制方案。该方案采用两个 32 - CHIP 的 PN 码，I、Q 通道的每个 PN 码采用 OQPSK 调制机制，码片采用半正弦脉冲波形。所用的 PN 码为 m-序列，m-序列是最大长度的线性反馈移位寄存器序列，理论完善成熟，在工程上容易实现，具有良好的伪随机特性。I 通道采用的 PN 码的特征多项式为 45（八进制），而 Q 通道采用的 PN 码特征多项式为 75（八进制），其符号率为 31.25kSymbols/s。

如图 7.9 所示，通过一个可能的移位值（共 16 个），周期性移位 PN 码，将信息放在每个通道的每个符号内。信息以差分方式放置在信道上，即信息是当前符号与其前一个符号的移位值的差。因为在一个符号传输时间内，$M=16$ 个移位值之一被放置在 I 和 Q 通道中的一个，则每个符号传输一个字节。这是因为，PN 码包含 32 个码片，理论上可以每个符号传送 5 个比特，但是实现较复杂，简单讲是由于将 8 个比特分为 4 个比特比分为 5 个比特更容易，而且较小的移位值简化了接收器的实现。

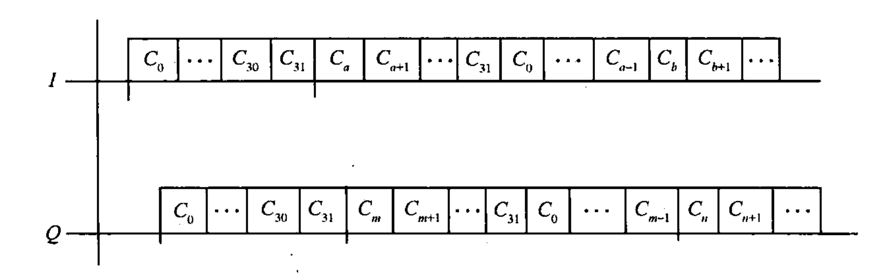


图 7.9　编码位置调制

传统的多级直序扩频需要为每个可能传输的序列产生不同的 PN 码。而该调制方案允许每个信道采用一个 PN 码，循环移位使用，简化了 PN 码的生成，降低了能耗。在很多集成电路中，PN 码的产生和存储增加了晶圆面积，因此该方案同时也节约了成本。

7.3.3.3　直序扩频 - 码分多址访问

C. Liu 与 H. Asada[15]提出了一种基于直序扩频—码分多址访问（DS-CDMA）的数据编码与调制方法。该方法采用最小能量（Minimum Energy，ME）编码，采用开关键控（On-Off-Keying，OOK）调制方法。OOK 是最简单的幅移键控，其载波在二进制调制信号控制下通断。在 OOK 中，高比特位（二进制中的 1）的传输耗能，低比特位（即二进制中的 0）传输不耗能，因此能量消耗由高比特的数目决定。如果在原有码字中加入一些冗余比特，则可以使用一套高比特位比例较小的码字来表示源符号，从而实现节能的目标，如图 7.10 所示。

最小能量编码的生成可分为编码本优化和编码优化两步，前者确定码字的集合（称为编码本），使编码本含有的高比特位数最少；后者使编码中含有的高比特位最少。表 7.4 给出了长度为 L 可用码字的集合，依据高位的数目排序，第 i 列为具有 $i-1$ 个高比特的码字。第 1 列为具有 0 个高比特的码字，共 $C_L^0=1$ 个；第 2 列为具有一个高比特的码字，共 $C_L^1=L$ 个；第 3 列有 C_L^2 个高位，依此类推。所有的码字从 1 到 2^L 编号，并按升序排

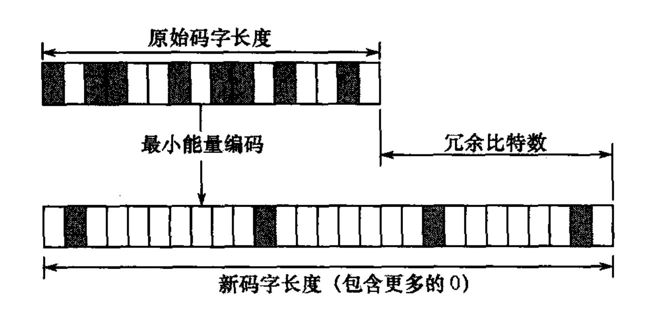


图7.10　最小能量编码的原理

列 $W_o=\{\omega_1,\cdots,\omega_{2^L}\}$，最后一个码字 ω_{2^L} 包含所有的高位，其传输耗能也最高。为了节能，不能使用包含很多高位的码字，而是使用前 q 个码字，抛弃其余的码字，如表7.5中折线所示。

表7.5　固定长度ME码字

码字	ω_1	$\omega_2\cdots\omega_{L+1}$	$\omega_{L+2}\cdots$	$\cdots\omega_q\cdots$	$\cdots\omega_{2^L-1}$	ω_{2^L}
码字数	C_L^0	C_L^1	C_L^2		C_L^{L-1}	C_L^L
码字模式						

采用ME编码的能量有效的DS-CDMA系统的配置如图7.11所示。数据源1～M采用冗余的ME编码，采用唯一的PN码扩展信号 $d_1(t)$ 的每个信道，然而PN码只应用于源码 $d_i(t)$ 的高比特位，而对于低比特位，没有扩展的信号产生。所有的信道信号经调制器调制后，接收端对接收到的信号进行解调，于是编码被恢复为源符号。

图7.11表示多个信号源的混合和调制。图中第 j 个接收器的数据信号 $d_j(t)$ 采用ME编码。值得注意的是，只为高比特位产生PN码，而低比特位没有信号生成，这与采用BPSK的CDMA不同。所提方案将多个通道的稀疏信号叠加，因此叠加多个非零信号的概率很低。图7.12显示多个非零信道信号很少重叠。系统可以同时发送多个非零信号，因此唯一的PN码可以分配给不同的信道，但是重叠的机会却降低了。随着信道数目的增加，干扰的机会会增加，但是可以通过增加ME的码长来克服这一缺陷，从而克服了标准CDMA随着信道数增加而干扰增加的缺陷。因此，该方法能够降低多路访问冲突，从而减少能量消耗。

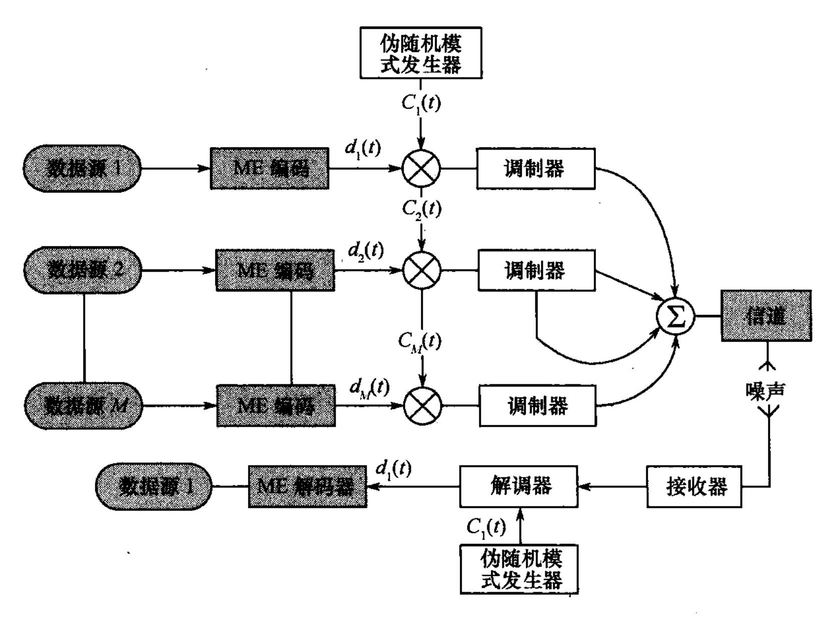


图 7.11　采用 ME 数据源编码的 DS-CDMA 系统框图

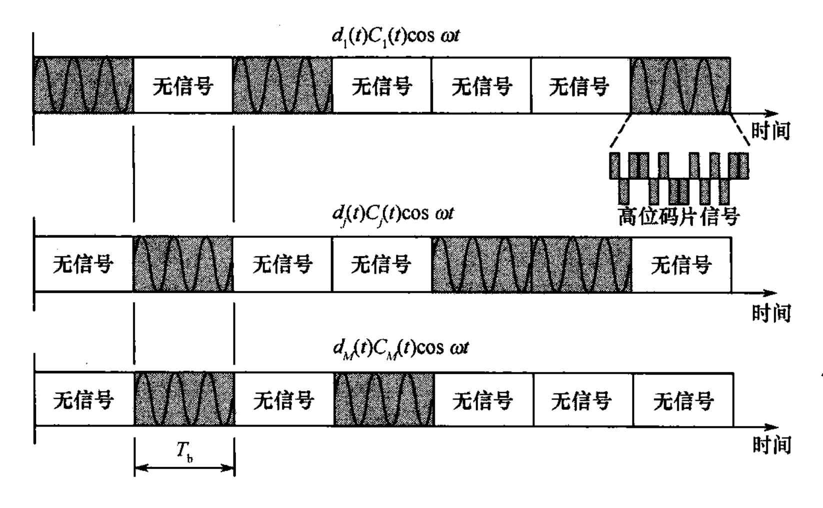


图 7.12　多接入冲突避免的原理

7.4　物理层面临的挑战与有待解决的问题

7.4.1　物理层面临的挑战[12]

无线传感器网络低能耗、低成本、小型化等要求给物理层的设计带来了很多困难，因此，有必要对其进行更多的研究和关注。本节介绍了无线通信的介质与频段选择、调制和扩频等关键技术，介绍了与无线传感器网络物理层协议相关的 IEEE802.15.4 标准和超宽带技术，概括与总结了无线传感器网络物理层协议设计的主要问题，详细描述了已有的

设计思路和解决策略。然而，人们对无线传感器网络物理层协议的研究还处于初级阶段，以下方面还需要做进一步的研究：

（1）扩频与调制机制。无线传感器网络规模大、密度高和带宽窄的特征使得其存在着严重的内部通信干扰，所以，无线传感器网络需要抗干扰能力强的扩频与调制方式。但是，由于传感器节点具有小型化、低成本、低功耗的特点和要求，所以同时又需要为其设计简单、低功耗的扩频与调制机制。因此，在设计扩频与调制机制时要能够很好地平衡其高效性和简单化。

（2）信号传播质量保障机制。由于无线传感器网络通常处于无人值守、未知的测控环境，无线通信经常会被障碍物或干扰源影响，出现信道丢失的情况，信号传播质量保障机制可以保障传感器节点间正常的数据传输。

（3）节能机制。μAMPS 只是简单描述和分析了状态转换的耗能问题，指出了活动状态与休眠状态之间的切换能耗不可忽略，但是转换模型过于简单，还不具有实际的指导意义，有待进一步探讨。另外，高效的电源模块是无线传感器网络广泛应用的前提，目前对于电源模块的研究仍然非常初步，待研究与实践。

（4）硬件方面。目前的无线传感器网络节点在体积、成本和功耗上与其广泛应用的要求还存在一定的差距，缺乏小型化、低成本、低功耗传感器节点的 SOC 实现以及以节能为目标的硬件管理策略。

7.4.2　物理层有待解决的问题

物理层负责数据的调制、发送与接收，是决定无线传感器网络的节点体积、成本以及能耗的关键环节，是无线传感器网络的研究重点之一。能耗和成本是无线传感器网络最主要的两个性能指标，也是无线传感器网络物理层协议设计中需要重点考虑和解决的主要问题[13~17]。

1. 能量问题

能量受限是无线传感器网络的重要特征，为了延长网络存活时间，物理层设计方案必须有效地利用能源。

无线传感器网络系统的平均能耗为

$$P_{avg} = U \cdot I_{AVG} \tag{7.30}$$

式中：U 为系统的工作电压；I_{AVG}为系统的平均电流。

系统的能耗又可以分为工作能耗和待机能耗两部分。

系统的平均电流为

$$I_{AVG} = T_{on} \cdot I_{on} + (1 - T_{on}) \cdot I_{stby} \tag{7.31}$$

式中：T_{on}为收发机启动时间占整个生存周期的百分比；I_{on}为系统在收发机启动时的电流；I_{stby}为系统在收发机待机时的电流。

【例 7.1】典型的 2.4GHz COMS 收发器发送时消耗能量 38mW，接收时消耗 32mW。为了进行对等网络负载周期的计算，简化接收机和发射机的能耗，皆取 35mW，而且假设通信链路是对称的，即发送和接收所需的时间是相等的。系统的工作电流和待机电流分别为 $I_{on}=17.5\text{mA}$ 和 $I_{stby}=30\mu\text{A}$，如果使用两个 750mA 的 AAA 电池串联供电，电压 $U=$

1.8V,为了满足电池一年约8760h寿命的目标,根据式(7.31)计算得到

$$I_{AVG} = 86\mu A$$

$$T_{on} = 0.27\%$$

由上可知,为了降低系统能耗,需要研究以下问题:

(1)无线传感器网络节点收发机的工作能耗远远大于待机能耗。减小 T_{on} 可以使活动节点尽快完成通信,返回睡眠状态,保证节点在低负载周期下运行,从而降低平均能耗。因此,如何减小 T_{on} 是无线传感器网络物理层设计需要解决的主要问题之一。

(2)收发机工作电流取决于符号率,而不取决于数据传输速率。于是,最小化符号率实现最小化的 I_{on} 也是设计的主要指标。因此,无线传感器网络物理层能耗的优化面临着降低符号率和提高数据传输速率的矛盾。

(3) T_{on} 还包括通信电路的启动时间。实际上,无线传感器网络系统通信时间非常短,所以,决定电源寿命的主要因素是启动时间。为了缩短启动时间,需要研究信道频率、基频的使用间隔以及窄带滤波器的使用。

无线传感器网络低能耗的要求同时也带来了能源选择问题。目前,无线传感器网络的主要能源仍然是传统的电池。但是如何根据无线传感器网络的工作特点选择合适的电池也是一个研究重点。同时,由于无线传感器网络无人值守的特点,一些可靠地从周围环境取得能量并将其转换成微瓦电能的方法受到了广泛的关注[18,19]。其中,振动和应变形式的光能、热能和机械能是最有可能的能量来源。然而,这些能源都有各自的局限性,例如,太阳能需要光照,机械能则需要动力。因此,无线传感器网络非传统能源的研究也是值得关注的问题。

2. 成本问题

成本是无线传感器网络广泛应用的前提,而决定硬件成本的物理层是决定网络成本的关键。为了降低成本,物理层的设计应该关注以下问题:

(1)集成化问题。无线传感器网络节点一般由传感模块、处理模块、通信模块和电源模块4个基本模块组成。传感模块包含传感器和模数转换器(ADC)两个子模块。传感器采集的模拟信号经过模数转换器转成数字信号后,传给处理模块,处理模块根据任务需求对数据进行预处理,并将结果通过通信模块送到网上。集成化的产品无需考虑其他外置部件,无疑可以降低成本。然而,对于无线传感器网络节点,电源和通信模块的天线是最难集成的元件,目前还没有理想的方案实现它们的集成。另一个较难集成的是石英晶体基频,在对基频的稳定性要求不高的离散条件下,可以考虑采用微电子机械系统(MEMS)共鸣器替代分立石英晶体振荡器。

(2)数字化问题。为了实现低成本集成,必须考虑模拟和数字电路的选择。众所周知,与模拟电路相比,数字电路的集成使用印刷电路板,体积较小、成本较低,因此尽可能采用数字电路是理想的方案。但是,在所有元件中,最难选择电路类型的是接收器的信道滤波器,如果采用模拟电路,则体积较大,而如果采用数字电路,则需要在其前增加一个假频滤波器和一个数模转换器,这个体积并未减小。由于模拟信道滤波器的大小与滤波器的转角频率成反比,因此,设计中应该考虑如何在信道滤波器的转角频率和IC成本之间取得折中。

(3)协议简单化问题。实现低成本要求采用简单的调制、解调和扩频算法,尽量降低所设计的协议、算法的复杂度,从而降低对硬件的要求。

参考文献

[1] Callaway E H. Wireless Sensor Networks:Architecture and Protocols[M]. Florida:CRC Press LLC, 2004:41 -62.

[2] Hac A. Wireless Sensor Network Designs[M]. NEW York:John Wiley&Sons, 2003.

[3] Francesca C, etc. Radio Resource Sharing for Ad Hoc Networking with UWB[J]. IEEE Journal on selected areas in communications,2002,20(7):1722 -1732.

[4] Pierre B, etc. Modeling and Optimization of UWB Communication Networks through a Flexible Cost Function[J]. IEEE Journal on Selected Areas in Communications,2002,20(7):1733 -1744.

[5] Naedis D, etc. UWB Ad -hoc Network[A]. IEEE Conference on Ultra Wideband Systems and Technologies(UWBST'02)[C], 2002:217 -223.

[6] Jin D etc. MAC Protocols for Ultra -Wide -Band(UWB) Wireless Networks:Impact of Channel Acquisition Time[A]. SPIE ITCOM Conf'02[C], 2002:48 -67.

[7] Zhang Z, Zeng F, Ge L. Correlation Properties of Time -Hopping Sequences for Impulse Radio[A]. ICASSP2003[C], 2003:141 -144.

[8] 唐岚,等. 超宽带无线传输技术[J]. 吉林大学学报(工学版), 2004,34(2):330 -335.

[9] 仇洪冰,等. 超宽带通信的调制及其信号特征[J]. 通信学报, 2003,24(B11):158 -165.

[10] 邵怀宗,等. 时间脉冲位置调制的超宽带无线通信[J]. 系统工程与电子技术, 2003,25(2):160 -164.

[11] Akyildiz I F, Su W, Sankarasubramaniam Y, etc. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38(4):373 -422.

[12] 张劼. 无线传感器网络体系结构及关键技术研究[D]. 西安:空军工程大学, 2007.

[13] Roundy S, Wright P K, Rabaey J M. Energy Scavening for Wireless Sensor Networks:With Special Focus on Vibrations [M]. Boston:Kluwer Academic Publishers, 2004.

[14] Favre P, etc. A 2V,600uA,1GHz BiCMOS Super Regenerative Receiver for ISM Applications[J]. IEEE Journal of Solid State Circuits,1998,33(12):2186 -2176.

[15] Melly T, etc. A 1.2V,430MHz,4dBm Power Amplifier and a 250uW Front End Using a Standard Digital CMOC Process [A]. IEEE International Symposium on Low Power Electronics and Design Coference'77[C]. 1999:233 -237.

[16] Shih E, etc. Physical Layer Driven Protocol and Algorithm Design for Energy -Efficient Wireless Sensor Networks[A]. Proc. ACM MobiCom'01[C], 2001:272 -286.

[17] Liu C, Asada H. A Source Coding and Modulation Method for Power Saving and Interference Reduction in DS -CDMA Sensor Network Systems[A]. Proceedings of the American Control Conference'02[C], 2002:8 -10.

[18] Rabaey J, Ammer M, Silva J, etc. PicoRadio Supports Ad Hoc Ultra -Low Power Wireless Networking[J]. IEEE Computer Magazine, 2002,33(7):42 -48.

[19] Chiasserini C F, Rao R R. Stochastic Battery Discharge in Portable Communication Devices[A]. 15th Annual Battery Conf. On Applications and Advances'2000[C], 2000:27 -32.

第8章　无线传感器网络MAC协议

数据链路层用于构建底层的基础网络结构，控制无线信道的合理使用，实现节点间链路的建立，保证所有的节点可以公平、有效地利用有限的带宽。如何控制信道接入是数据链路层MAC子层的主要任务，MAC子层决定节点如何接入共享的无线信道，并负责向上层提供可靠的点到点通信链路。在MAC层，减少节点能量消耗的主要措施是减少数据发送的冲突，避免重传[1]，同时使节点在适当的时候进入休眠状态。

传统的无线网络，如GSM和CDMA中的MAC协议，主要关心如何满足用户QoS要求，包括网络吞吐率、带宽利用率、实时性和公平性等，能耗是第二位的；Ad hoc网络则考虑如何在节点具有高度移动性的环境中建立彼此间的链接，同时兼顾一定的QoS要求，能耗也不是首要关心的；蓝牙采用了主从式的星型拓扑结构，这本身就不适合传感器网络自组织的特点[2]。

无线传感器网络MAC协议是保证无线传感器网络高效通信的关键网络协议之一。无线传感器网络的性能，如吞吐量、延迟性能等在较大程度上取决于所采用的MAC协议。因此，设计性能优越的MAC协议算法成为无线传感器网络研究的一个热点问题。

8.1　无线传感器网络MAC协议概述

无线频谱是无线移动通信的通信介质，是一种广播介质，属于稀缺资源。在无线传感器网络中，可能会有多个节点设备同时接入信道，导致分组之间相互冲突，使接收方无法分辨出接收到的数据，浪费信道资源，吞吐量显著下降。为了解决这些问题，就需要媒体介质访问控制（Medium Access Control，MAC）协议。所谓MAC协议，就是通过一组规则和过程来更有效、有序和公平地使用共享介质。MAC协议处于无线传感器网络协议的底层部分，主要用于在传感器节点间公平有效地共享通信媒介，该协议位于无线传感器网络层次协议中数据链路层的下半部分，主要负责控制与连接物理层的物理介质。在发送数据的时候，MAC协议可以事先判断是否可以发送数据，如果可以发送将给数据加上一些控制信息，最终将数据以及控制信息以规定的格式发送到物理层；在接收数据的时候，MAC协议首先判断输入的信息是否发生传输错误，如果没有错误，则去掉控制信息发送至LLC层。

MAC协议是影响无线传感器网络能量消耗的重要因素，无线传感器网络MAC协议关注的核心问题是能耗。无线传感器网络中，造成能耗因素有很多。其中，射频通信模块是能耗最大的部件，而MAC协议直接控制射频通信模块，对无线传感器网络节能具有重要影响。MAC协议能耗的主要包括以下4个方面[3]：

（1）空闲侦听（Idle Listening）。节点不能预知它的邻居节点何时传输数据给自己时，

射频模块一直保持为接收模式。而且,节点在不需要发送数据时,也一直保持对信道的空闲侦听,过度空闲侦听或没必要的空闲侦听会造成节点能量浪费。这是能量浪费的主要因素。此外,如果控制消息过多,也会消耗较多的能量。

(2)冲突重传(Collision and Retransmission)。节点在发送数据过程中,在竞争共享的无线信道时,多个邻节点向同一节点发送数据产生碰撞,信号相互干扰,数据包发送失败,接收方无法准确接收,这就浪费了发送和接收数据上的能量,而重发数据则消耗节点更多的能量。

(3)串扰(Overhearing)。数据包是在共享的无线信道中传输,节点可能会接收和处理无关的、不必要的数据(不是发送给自己的数据包)。这种串音现象造成节点的无线接收模块和处理模块消耗更多的能量。

(4)控制报文开销(Control Packet Overhead)。MAC 协议首部包括一些控制信息,如 RTS/CTS/ACK,控制报文只包含节点间的协商数据,不传送有效数据。引入控制报文虽可提高通信可靠性,但需要消耗一定的能量。

在以上 4 种能耗来源中,空闲侦听的能耗占绝对大的比例,特别是在消息传输频率较低的情况下。传感器节点无线通信模块的状态包括发送、接收、侦听和休眠 4 种状态,目前的 MAC 协议在降低功耗方面主要集中在增加节点的休眠时间,减少节点对信道的空闲侦听。

无线传感器网络的 MAC 协议可采用基于预先规划的机制来保护节点的能量。其中,射频通信模块是节点中最大的耗能模块,是 MAC 协议优化的主要目标。MAC 协议在降低功耗方面主要采用的方法有减少数据流量、增加射频通信模块休眠时间和冲突避免等。具体来说,有以下几个方面:

(1)MAC 协议直接控制射频模块,对节点功耗有重要影响。节点在没有数据接发时,关闭射频模块,转入休眠状态,这种方法可以降低工作占空比,减少串扰和空闲侦听带来的能量浪费,代价是增加延迟和降低系统的吞吐率。

(2)减少数据流量主要靠在网络层或者在数据链路层上增加一个数据融合层来实现。

(3)节点在没有数据收发时,关闭射频模块,转入休眠状态。这种方法可以降低工作占空比,减少串扰和空闲侦听带来的能量浪费,代价是增加延迟和降低系统的吞吐率。

8.2 典型 MAC 协议分析

文献[4]将无线传感器网络 MAC 协议分为非调度式(Unscheduled MAC)和调度式(Scheduled MAC)两大类。本节根据信道分配使用方式,将无线传感器网络 MAC 协议分为基于无线信道随机竞争方式、时分复用方式、无线信道时分/频分/码分等混合复用接入方式 3 种,具体包括多收发器式、调度式、非调度式、混合式和基于跨层设计等 5 种类型。

(1)随机竞争接入方式。节点需要发送数据时采用随机方式使用无线信道,典型的如采用载波监听多路访问 CSMA 的 MAC 协议,需要注意隐藏终端和暴露终端问题,尽量减少节点间的干扰。

(2)时分复用无竞争接入方式。采用时分复用(TDMA)方式给每个节点分配了一个固定的无线信道使用时段,可以有效避免节点间的干扰。

(3)时分/频分/码分等混合复用接入方式(TDMA/FDMA/CDMA)。通过混合采用时分和频分或码分等复用方式,实现节点间的无冲突信道分配策略。

8.2.1　多收发器式 MAC 协议

PAMAS(Power Aware Multi Access with Signaling)[5]是最初为 Ad hoc 网络设计的一种 MAC 协议,利用两个收发器达到节能的目的。一个用于收发数据,一个用于收发控制消息,以防止数据冲突,减少重传和串扰引起的能耗。

PAMAS 协议的数据传输过程如图 8.1 所示。在未进行任何载波侦听的情况下,发送节点通过控制信道向接收节点发送 RTS 消息。接收节点先检查自身的控制信道和数据信道是否空闲:若空闲,则通过控制信道向发送节点返回 CTS 消息;若发送节点在规定的时间内未收到接收节点返回的 CTS 消息,则利用二进制指数回退方式进入回退模式。一旦发送节点收到 CTS 消息,便利用其数据信道传输数据包。接收节点在接收数据包过程中,通过控制信道发出长度为 RTS 和 CTS 的两倍的忙音,以便让邻节点知道数据信道已被占用。此外,当接收节点的控制信道出现噪声或收到其他节点的 RTS 消息时,都通过控制信道发出忙音,防止邻节点被激活。

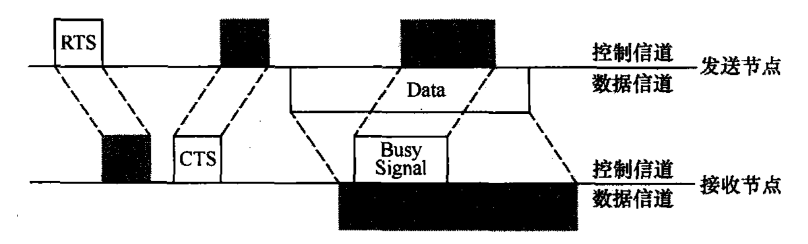


图 8.1　PAMAS 协议数据传输过程

虽然 PAMAS 协议采用两种信道分别传输控制消息和数据消息,可有效防止数据冲突,减少重传和串扰等问题。其缺点也很明显,例如,若存在隐终端问题,节点 A 和节点 C 之间无法直接通信,不知道彼此的工作状态,节点 B 向节点 A 正常的数据发送可能会被破坏。当节点 A 和节点 C 都收到发送节点 B 的 RTS 消息,且节点 C 的数据信道正在接收其他节点的数据,则节点 C 会向节点 B 返回忙音,这会和节点 A 的 CTS 消息重叠。由于忙音的长度大于 CTS 消息,使节点 A 的 CTS 消息遭到破坏,进而节点 B 不能启动数据发送过程。该过程如图 8.2 所示。

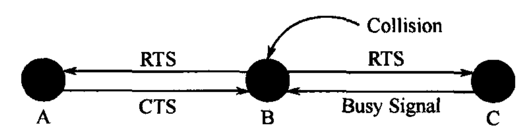


图 8.2　PAMAS 协议未解决隐终端问题

此外,PAMAS 协议需要在节点上安装两个收发器,这会增加节点的成本和体积。

由于信道损失的原因,加上任何收发器都存在一个最小接收信号强度的阈值,因此,节点都存在一个其发射信号能够覆盖的有效工作范围。如果发送节点和接收节点的距离

超出有效工作范围，可能导致隐终端（Hidden - terminal）和显终端（Exposed - terminal）问题[3]。

隐终端问题常发生于载波侦听多点接入（CSMA）协议中，在这种情况下，节点在开始发送数据包前要检测媒介的状态。若媒介处于忙的状态，节点则推迟数据包的发送，以避免发生碰撞。

如图 8.3 所示，假设节点 A 和节点 B、节点 B 和节点 C 在彼此的通信范围内，但节点 A 和节点 C 不存在交叉区域，即二者不能直接通信。节点 A 开始发送数据包到节点 B，一段时间后节点 C 也开始向节点 B 发送数据包。由于节点 C 无法接收节点 A 的信号，因此节点 C 的载波侦听功能错误地报告媒介处于空闲状态。当节点 C 发送其数据包至节点 B 时，会和节点 A 发送至节点 B 的数据包相碰撞，使二者的数据均变为无用的数据。在隐终端情况下，使用简单的 CSMA 协议有可能会导致数据包的碰撞。

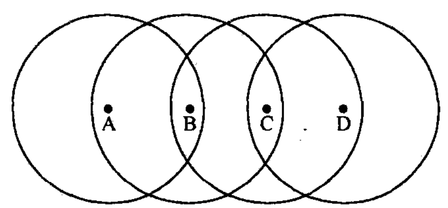


图 8.3　隐终端与显终端问题示意图

在显终端情形下，节点 B 向节点 A 发送一个数据包，一段时间后，节点 C 开始发送数据包至节点 D。尽管在理论上这种发送是可行的，即节点 A 和节点 D 都能收到数据包而没有失真，但节点 C 的载波侦听功能会抑制节点 C 的发送，从而使信道资源浪费。

8.2.2 调度式 MAC 协议

S-MAC（Sensor MAC）协议[6]是一种被广泛研究的调度式 MAC 协议，它通过同步邻节点睡眠调度的方式形成虚拟簇。节点在每一帧的开始，周期性地传输 SYNC 消息。据此，节点可知道邻节点的调度，以便在合适的时候被唤醒，如图 8.4（a）所示。

S-MAC 协议采用 RTS/CTS/DATA/ACK 机制发送数据，利用物理和虚拟载波侦听机制减少冲突和串扰。与 IEEE802.11 协议不同，当邻节点在通信时，节点直接进入休眠状态；当接收节点空闲并正在侦听周期时，才会被唤醒。

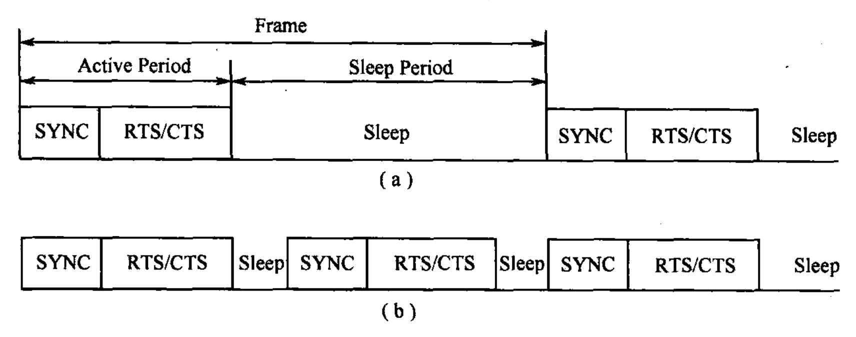


图 8.4　S-MAC 和 DSMAC 协议调度格式

（a）S-MAC 协议调度格式；（b）DSMAC 协议调度格式。

对于多跳无线传感器网络，节点周期性休眠会导致通信延迟的累积。针对此，S-MAC协议运用流量自适应侦听机制，减小通信延迟的累加效应。其基本思想如下：在一次通信过程中，邻节点在通信结束后，不立即进入休眠状态，而是保持侦听一段时间。如果节点在该时间段内收到 RTS 消息，则立即接收数据，无需进入下一次侦听周期，减少了数据包的传输延迟；如果该时间段内未收到 RTS 消息，则转入睡眠阶段，直到下一次侦听周期。

S-MAC 协议的缺点在于占空比为静态的，无法结合流量动态调整占空比；对虚拟簇的大小也没有限制，大规模的簇会带来较大的网络延迟。

DSMAC(Dynamic Sensor MAC)协议[7]在 S-MAC 的基础上，对占空比与流量的适应性进行了改进，使占空比可根据流量与节点能量动态调整。在 SYNC 同步期间，所有节点共享一跳的延迟值，但平均每跳延迟增大时，节点工作的占空比相应增加；当流量降低到较低水平时，减小占空比。图 8.4(b)给出了 DSMAC 协议占空比加倍的原理。

T-MAC(Timeout-MAC)协议[8]利用定时器 TA，而非占空比式调度确定侦听阶段的结束。T-MAC 协议定义了 5 种事件和 1 个定时器 TA，据此决定工作阶段的结束时间。这 5 种事件分别为帧长度超时；节点在无线信道收到数据；数据传输发生冲突；节点数据或确定发送成功；邻节点完成数据交换。

如果在 TA 时间内，射频模块未侦听到这 5 种事件中的任何一种，则认为信道空闲，关闭射频模块，进入休眠状态。T-MAC 协议结构如图 8.5 所示。

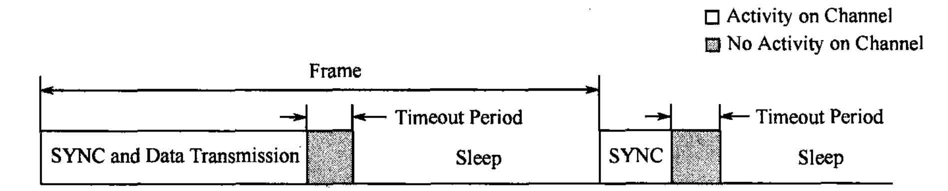


图 8.5　T-MAC 协议结构

尽管 T-MAC 协议能根据流量动态调整占空比，提高了能量利用率，但存在一种特殊的通信延迟，即早睡问题(Early - sleep Problem)，早睡原理如图 8.6 所示。通过引入 FRTS 和 DS 格式数据包可减小早睡问题发生的可能性，起到控制网络流量的作用，但又

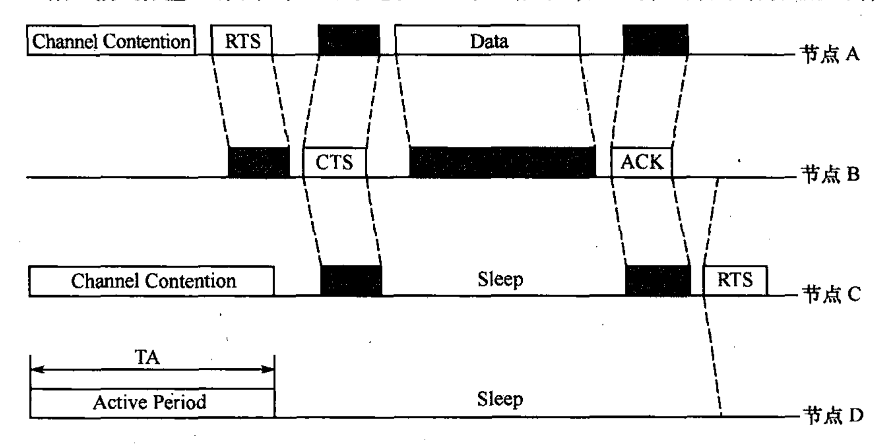


图 8.6　T-MAC 协议早睡问题

会增加网络冲突的可能性。

TLTS(Two Level TDMA Schedule)协议[9]是一种基于簇的 TDMA 协议,通过两级 TDMA 调度,避免簇间和簇内的干扰。

该协议首先为各个相邻的簇分配不同的帧号,以避免簇间传输干扰;其次,簇头根据 TDMA 调度,给成员节点分配不同的时隙。此外,TLTS 协议利用簇内覆盖的思想,选取簇内部分节点作为工作节点,其他的则处于休眠状态,以减少 TDMA 超帧的长度,减少数据包的延迟和网络能耗。TLTS 协议的缺点在于网络规模很大或簇数目较多时,超帧的长度过大,会带来较大的网络延迟。

8.2.3 非调度式 MAC 协议

B-MAC(Berkeley MAC)协议[10]是一种非调度式 MAC 协议,各节点根据独立的占空比进行工作状态的转换,并采用较长的唤醒前导进行消息传递。这样,周期性的侦听信道的接收节点有足够的时间被唤醒。B-MAC 协议依赖于对信道状态的精确估计,可利用滤波机制增加对信道估计的可靠性,B-MAC 协议结构如图 8.7 所示。

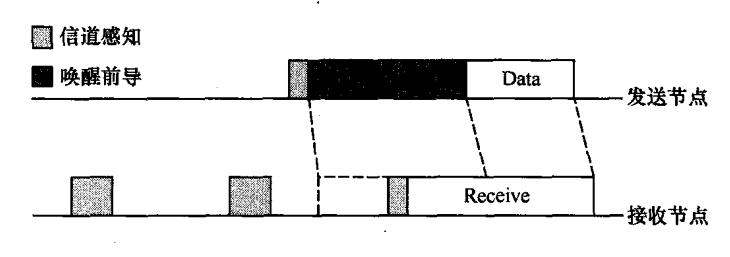


图 8.7 B-MAC 协议结构

WiseMAC(Wireless Sensor MAC)协议[11]对 B-MAC 协议中的唤醒前导进行改进,减少唤醒前导的长度,进而减小控制开销。WiseMAC 协议在 ACK 中携带了下一次信道侦听的时间,节点可获得所有邻节点信道侦听时间,在发送数据时,对唤醒前导进行压缩。WiseMAC 协议结构如图 8.8 所示。

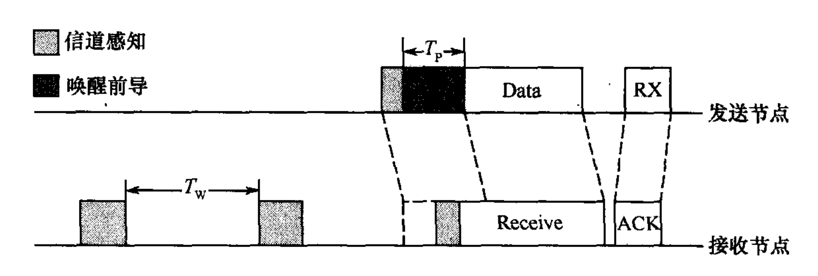


图 8.8 WiseMAC 协议结构

文献[11]结合节点时钟漂移系数和侦听周期,得出唤醒前导长度为

$$T_P = \min(4\theta l, T_w) \tag{8.1}$$

式中:θ 为节点时钟漂移系数;l 为上次发送 ACK 到当前的时间间隔;T_w 为侦听周期。

WiseMAC 协议也存在诸多缺点,如节点需要存储邻节点的侦听时间,对高密度网络

而言，由于计算量大引起的延迟较严重；另外，隐终端问题也未得到很好的解决。

TRAMA(TRaffic Adaptive MAC Protocol)[12]是流量自适应的MAC协议，旨在提高传统的TDMA能量利用率。TRAMA协议由邻居协议NP、调度交换协议SEP和自适应选举算法AEA三部分组成，并在假定所有节点时间同步的基础上，将时间划分为随机接入时段(Random Access Periods)和调度访问接入时段(Schedule Access Periods)，如图8.9所示。

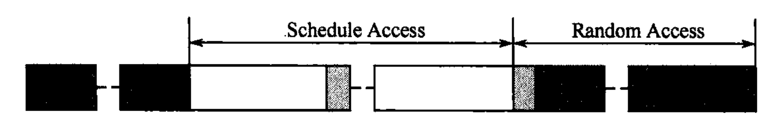


图8.9　TRAMA协议调度格式

邻居协议NP仅在随机接入时段执行，这个时段被划分为若干个小的时隙。节点随机选取一些时隙传输控制消息，而不进行载波侦听。控制消息包含节点ID、上一周期新节点的加入和已有节点的死亡等拓扑变化信息。在该过程中，所有节点都处于工作状态。

调度交换协议SEP用来建立和维护调度信息。在调度阶段，节点周期性广播调度信息。调度过程如下：节点根据应用层数据包的速率，计算调度间隔$T_{INTERVAL}$(一次调度对应的时隙数)，然后计算在$[t, t+T_{INTERVAL}]$时间段和两跳内邻节点中优先级最高的时隙数。最后，在优先级最高的时隙内发送数据，并通过调度消息告诉对应的接收方。节点A在编号为t的时隙内优先级计算公式为：

$$\text{Priority}(A, t) = \text{Hash}(A \oplus t) \tag{8.2}$$

如果节点无足够多的数据包需发送，应及时放弃该时隙以供其他节点使用。此外，在每个调度间隔内，为防止调度信息不一致和发送调度数据包时产生冲突，最后一个最高优先级时隙预留给节点广播其下一个调度间隔的调度信息。

自适应选举算法AEA根据当前两跳邻节点的优先级和一跳邻节点调度信息，决定节点在当前时隙的状态，如接收、发送或休眠。在调度时段的每个时隙上都要运行AEA算法。

尽管TRAMA协议能量有效性较高，并可基于流量自适应调整调度，避免信道资源的浪费。和WiseMAC协议类似，当网络中节点密度较大时，TRAMA协议需要较多的存储空间，以保存两跳内的拓扑信息，包括邻节点列表和节点调度。

IEEE802.15.4协议[13]是用于小型、低功耗和低传输速率无线传感器网络的MAC协议。与IEEE802.11类似，包括星形拓扑的集中式结构和P2P拓扑的分布式结构，但无论哪种结构，网络中都包含一个PAN协调器。对于星形结构，所有的通信都经过PAN协调器；P2P结构中的节点可独立运行，无需经过PAN协调器，但节点在接入网络前必须和PAN协调器关联。

IEEE802.15.4协议的信道接入过程：节点在监测信道前，执行随机回退算法，若信道空闲且采用非时隙CSMA/CA，则可立即传输数据包；若节点采用时隙CSMA/CA，等待到下一个时隙，并监测信道，如果初始回退周期后的两个保守时隙内信道都空闲，则进行数据包的传输。一旦监测到信道忙，执行回退算法。

IEEE802.15.4 协议的数据传输过程如图 8.10 所示。

发送节点　PAN 协调器　接收节点

Data　Data Request　ACK　ACK　Data　ACK

图 8.10　IEEE802.15.4 协议数据传输过程

8.2.4　混合式 MAC 协议

Z-MAC(Zebra - MAC)[14]协议是一种综合利用 TDMA 和 CSMA 协议优点的混合式 MAC 协议,其基本原理在于根据信道竞争激烈程度在 TDMA 和 CSMA 之间切换工作方式:当信道竞争激烈或网络流量大时,节点利用 TDMA 方式共享信道;当信道竞争不激烈或网络流量小时,节点以 CSMA 方式竞争信道。换言之,节点在属于自己的时隙内有数据包需要发送时,则占用该时隙;当节点在属于自己的时隙内由于故障、死亡或无数据包需要发送时,其他节点可以占用该时隙。

Z-MAC 协议在建立阶段依次运行“邻节点发现”、“时隙分配”、“局部帧交换”和“全局时钟同步”操作。研究表明:该协议对时钟同步误差、时隙分配失败以及时变的信道质量具有鲁棒性;但在“邻节点发现”操作中,需要知道一跳内邻节点列表,并以此推断两跳内邻节点列表作为“时隙分配”操作的输入,这会占用节点一定的存储和计算资源。

S. Waharte 等人[15]针对分簇型网络簇间覆盖区域重叠并引起簇间传输干扰的问题,提出节点在簇内按 TDMA 方式调度,相邻簇间则按 FDMA 方式使用不同频带通信,以减少簇间干扰。频带分配问题是个 NP 难问题,可用图着色理论来建模;但簇间采用 FDMA 共享信道时,要求节点支持多种工作频率,目前市场上大部分节点的工作频带比较单一[16]。

8.2.5　基于跨层设计的 MAC 协议

跨层设计通过层与层之间的信息交换来满足全局需要,其优点在于层与层之间的信息共享提高了各层的适应性,使整个网络的性能得到提高。在满足能量受限情况下,满足应用的高吞吐量、低延迟等要求。

CAEM(Channel Adaptive Energy Management)协议[17]是一种结合物理层和 MAC 层设计的跨层协议。在该协议中,每个节点具有控制信道和数据信道,簇头通过控制道发送周期脉冲,节点根据收到的脉冲判断当前信道质量以及数据信道是否空闲。簇中节点分为监测信道、休眠传输以及回避状态,由于休眠状态节点耗能很少,而节点处于监测状态是仅工作于能耗较少的控制信道,从而可以节约大量能量。节点有数据需要发送时,首先根据控制信道监测无线链路的信道质量,当信道空闲且信道质量优于阈

值时,节点发送数据并且节点可以根据信道的质量不同,在物理层采用不同的调制方式,以提高信道的利用率。节点发送完数据后,进入休眠状态,直至有数据需要发送时才进入监测信道状态。

在CAEM协议中,数据只在链路质量好的时候发送,故其可减少数据传送和接收的时间,从而节省了能量。数据在链路质量不好时,会把数据保存在数据缓存中,这样会增加数据包的延迟和数据包溢出丢失。此协议最大的缺点在于有些节点如果一直处于链路质量不好的状态,它将一直没有工作机会,导致节点利用率的极度不公平。

CuMPE(Cluster - Management and Power - Efficient Protocol)协议[18]是一种结合MAC层和路由层的协议。在路由层,该协议用选择性泛洪算法传播消息,用贪婪算法选择节点和簇头之间能耗最小的路径。在MAC层,该协议采用TDMA机制找出路由树中最重要的路径并在不增加路径的条件下,调度节点发送消息。CuMPE协议主要由4个阶段构成:

(1)选择上游能耗最少的节点作为簇头。

(2)选择单跳路径传输数据代替多跳传输。

(3)找出簇树结构中的关键路径,即是簇树结构中最长的路径。

(4)按照TDMA机制,每个节点向上游邻节点发送数据。

CuMPE协议可有效的节省能量,网络延迟短,但信道利用率低。

8.2.6 典型MAC协议性能比较

表8.1对本章给出的几种典型MAC协议的性能进行比较。不难看出,大多数协议只是在某一方面有较好的性能,如能量有效性高、网络延迟短等,总体性能则一般。

表8.1 典型MAC协议性能比较

协议	时间同步	信道数	平面/分簇	空闲侦听避免方法	串扰避免方法	数据冲突避免方法	扩展性
PAMAS	无需	2	二者	—	双信道	RTS/CTS 忙音	好
S-MAC/DSMAC	需要	1	平面	周期性休眠	NAV	RTS/CTS/ACK	一般
T-MAC	无需	1	平面	TA	—	RTS/CTS/ACK	好
TLTS	需要	1	分簇	周期性休眠	—	超帧	一般
B-MAC	无需	1	二者	周期性侦听	唤醒前导	RTS/CTS/ACK	好
WiseMAC	无需	1	二者	周期性侦听	唤醒前导	RTS/CTS/ACK	好
TRAMA	需要	1	平面	时间表	时间表	时间表	一般
IEEE802.15.4	无需	1	二者	PAN 协调器	PAN 协调器	RTS/CTS/ACK	一般
Z-MAC	需要	1	二者	周期性休眠	—	CSMA	好
S. Waharte	需要	n	分簇	周期性休眠	FDMA	TDMA 调度	一般
CAEM	无需	2	分簇	—	信道质量估计	—	好
CuMPE	需要	1	分簇	周期性休眠	—	—	一般

基于竞争机制的MAC协议很难保证实时性,在主要考虑节能而不太关心时延的场合有较大的应用。而且由于冲突的存在,需要重发或反复监听,浪费了能源。根据这类协议

“分布式和随机补偿”的特性，基于竞争的协议没有确切地保证不同节点的数据帧的优先级。

非冲突的 MAC 协议通过消除冲突来节能。好的非冲突协议能够潜在地提高吞吐量，减少时延，提供实时性保证。存在的问题是多信道的使用，这对无线传感器网络的节点硬件设计上提出了一个附加的要求：节点必须有两个收发器。对于硬件成本增加与能耗节省之间的平衡关系需要进行评估，以便确定是否采用该类协议。另一个问题是协议的复杂性。因为节点的计算能力有限，传感器网络的协议总是越简单越好。

基于调度机制的 MAC 协议均是分布式协议，需要时间同步机制。由于不需要全局的有关信息，在网络拓扑改变的情况下可充分适应并保持最佳的特性。这类协议提供了信道的公平使用，与合适的调度算法配合就可避免冲突的发生，较适用于无线传感器网络。该类协议主要使用的调度算法是时分多复用（TDMA），即将时间分成多个时隙，几个时隙组成一个帧，在每一帧中，分配给节点至少一个时隙来发送数据。这类协议的调度算法通常寻找一个尽可能最近的用于发送数据的帧来达到高的空间利用率和低的数据帧等待时间。

8.3 无线传感器网络 MAC 协议设计策略

无线传感器网络是应用相关的网络，不同应用对 MAC 协议的考虑也不尽相同。虽然正有越来越多的适用于无线传感器网络的 MAC 协议被提出，但这些协议只是部分的满足无线传感器网络的性能要求，或只是针对特定的应用需求，不具有通用性。MAC 协议设计时，需要着重考虑以下 3 个方面[3]。

（1）能量有效性（Energy Efficiency）。由于网络节点数量以及放置环境等因素影响，越来越趋向使用一次性电池，节点一般是以干电池、纽扣电池等提供能量，电池能量通常难以补充，MAC 协议在满足应用要求前提下，应尽量节省和高效地使用节点的能量，即让传感器节点尽可能地处于休眠状态，以减少在通信时的能耗。

（2）可扩展性（Scalability）。节点数目、节点分布的密集程度和网络拓扑结构要具有可扩展性，以适应网络中节点个数增加或者减少和位置等变化。因此，MAC 协议应具有可扩展性，以适应拓扑结构的动态性。可扩展性传感器网络中网络节点数目一般较大。

（3）兼顾网络性能。网络性能包括网络的公平性、实时性、网络吞吐量以及带宽利用率等。不同应用的传感器网络产生不同特征的流量，要求不同的性能参数，所以 MAC 协议应能兼顾好这些网络性能。

在设计 MAC 协议时，上述 3 个方面的重要性依次递减。此外，不仅应该注意以上几个方面，更重要的是在这些衡量标准中取得一个很好的平衡。普遍认为，节约能量是 MAC 协议设计的首要目标，其他性能视具体应用决定。为了达到首要性能可以适当地牺牲部分次要的性能。

无线传感器网络 MAC 协议除了要减少空闲侦听、数据冲突、串扰和控制报文开销引起的能耗外，还存在如下几个问题：

（1）对时间同步的敏感性。基于 TDMA 的调度式 MAC 协议要求节点能够时钟同步，

当节点时钟漂移时，采取何种方法削弱不同步引起的 MAC 协议性能下降是 MAC 协议存在的问题之一。

(2)对网络拓扑结构变化的适应性。许多 MAC 协议要求知道两跳内邻节点属性(如节点 ID、位置等)，并将这些属性以 Table 或 List 的形式保存在节点的存储器中。当网络拓扑结构发生变化时，需要借助拓扑发现算法获取上述属性。这个过程既会带来网络的延迟，又会占用大量的存储空间，这也是 MAC 协议存在的问题之一。

(3)对网络流量和信道质量的适应性。由于无线传感器网络的网络流量和信道质量有较强的时变特性，对于连续监测型、事件驱动型和查询型网络，其流量特征各异。如何设计合理的 MAC 协议，能适应网络流量和信道质量的变化，是 MAC 协议存在的又一问题。

今后，无线传感器网络 MAC 协议在以下几个方面有待进一步发展：

(1)在能量有效性的基础上，提高 MAC 协议对网络流量和拓扑结构的适应性。

(2)运用跨层设计思想，综合提高网络性能，包括 MAC 层与路由层、物理层与应用层的资源共享。

(3)提高 MAC 协议对 QoS 的支持。随着视频或图像传感器接入无线传感器网络，在能量有效性较高的基础上提高 MAC 协议对 QoS 的支持，有助于视频传感器网络在目标跟踪、交通安全等领域发挥巨大作用。

8.4　基于动态非等分时隙的 MAC 协议

为了解决网络中节点空闲侦听、冲突、串听和控制开销所带来的无效功耗，并保证 MAC 层在相互竞争的用户之间分配信道资源，提供可靠的点到点通信链路，保证节点可以公平、有效地利用有限的带宽。目前，基于 TDMA 方式设计的协议仍存在一些不足[19]：

(1)一些 TDMA 协议采用全局信息来进行调度，使得节点数量较大的无线传感器网络要获取全局信息代价过于昂贵，且可扩展性受到局限。

(2)有些 TDMA 协议仍然存在冲突，浪费了能量，并且很难控制这些冲突来保证实时性，使得能耗有效性受到损害。

(3)对于时隙的分配不够严密，属于不同子网的节点可能得不到通信机会。

为了克服 TDMA 协议的不足，设计基于 TDMA 方式的非等分时隙能耗有效的选举 MAC 协议(Asymmetry - Slot Voting Media - Access Control，ASVMAC)。下面分别从相关定义、算法描述、算法设计和能耗有效性分析 4 个部分详细介绍 ASVMAC 协议。

8.4.1　ASVMAC 协议相关定义

【定义 8.1】回合：传感器节点将一组感知数据发送，直到 Sink 节点接收完毕为一个回合。

【定义 8.2】元数据(metadata)：描述节点自身属性的数据，如节点 ID 号、位置、剩余能量、故障诊断结果等。

【定义 8.3】时间基准：以节点容量最大的簇内时隙为起始时隙，以完成数据上传的容量最小簇内节点时隙为终止时隙，以终止时隙时间作为第 2 层簇头节点与 Sink 节点通信

起始时间基准,完成第 2 层的数据传输。

【定义 8.4】局部时序:基于 2 层的拓扑结构,将回合时间划分为簇内和簇间两大部分,各个簇内部以同一时间基准开始自己独立时隙内的通信,互不干扰,簇内通信完毕,簇头再以划分的不等分时隙完成第 2 层的通信。时间调度在各层中分别完成,不需要全局时序信息。

8.4.2　ASVMAC 协议总体描述

无线传感器网络对消息延迟的要求不高,在许多应用系统中,延迟几秒甚至几分钟都是可以接受的,而且 TDMA 协议较之 FDMA 具有抗干扰能力强,频率利用率高和系统容量大的优势,且相对其他协议如 CDMA、CSMA/CA 是最简单最容易实现的。ASVMAC 一方面采用局部时序信息进行调度,不需要全局范围内的时间同步,减少了控制帧的数量,降低了网络的通信负载,每个节点在分配的相应时隙内发送数据,避免了节点通信冲突。通过为簇头节点不等分时隙,既可以提高时隙利用效率,又可使大多数节点没有数据发送时进入低功耗运行模式。另一方面采用簇内节点选举机制,选举剩余能量最低的节点为休眠节点,邻节点只需监听一段时间之后使无线通信模块进入掉电模式,一定程度上降低了网络系统的能耗。

ASVMAC 协议属于调度类协议,借鉴 DE - MAC 协议设计思想,采用了周期性监听和休眠机制,而周期性监听有利于网络可扩展性的实现。由于本文是在 2 层分簇拓扑结构基础上研究无线传感器网络的,因此网络节点部署后,由 Sink 节点发起,进行网络拓扑发现和建立。首先由预先指定的簇头节点形成规模不等的簇,收集簇内传感器节点的数量信息上报给 Sink 节点,Sink 节点负责把传感器节点时隙数量及时隙大小的基本信息广播给各个簇头节点,各簇头节点按局部时序原则,分配各自网络时隙大小,并上报给 Sink 节点,同时将初始化 TDMA 调度表发给簇内每个节点和所有簇头节点,所有节点都在本地保存一个 TDMA 调度表,从而知道其邻节点将在哪个时隙上发送数据帧。所有簇头节点保存一个时间基准,在网络拓扑不变的情况下,始终以这一基准完成第 2 层时隙数据的传送,当拓扑改变后,则依据重建的调度表再建立一个“时间基准”。

8.4.3　非等分时隙协议设计与选举算法

1. ASVMAC 协议帧定义

ASVMAC 协议帧分为数据帧(Data Frame, DF)、控制帧(Control Frame, CF)。DF 是节点本身产生的或其他节点传送过来的需要路由到 Sink 节点的数据帧。根据在网络平台上的反复调试,保证正确传输数据,且代码量最少的前提下,DF 帧格式设计如图 8.11 所示。其中,包括 2B 数据帧类型标识(用于将数据帧与控制帧区分开来),1B 数据帧总长度,1B 传感器节点 ID 号,4B 系统时间,2B 的字节地址,4B 采集数据、1B 累加和校验、1B 帧尾标识。

类型标识	数据长度	节点 ID	系统时间	字节地址	数据内容	和校验	帧尾标识
2B	1B	1B	4B	2B	4B	1B	1B

图 8.11　数据帧的定义

每个控制帧包括:1B 的控制帧类型(Type Identifier,TI);1B 的所在簇 ID 号(Cluster Identifier,CI);若干字节的控制帧数据(Data Identifier,DI),CI 定义如图 8.12 所示。

类型标识	节点ID	数据长度
1B	1B	<4B

图 8.12　控制帧定义

ASVMAC 协议控制帧分为调度帧(Scheduling Frame, SF)和选举帧(Vote Frame, VF)。

调度帧用于网络初始化阶段形成调度表,包括 ID 请求帧(ID Request Frame, IRF)、ID 发送帧(ID Sending Frame, ISF)和调度表发送帧(Table Sending Frame, TSF)。

(1) IRF(TI=1)。簇头节点 i 发送 IRF 给它的邻传感器节点,用于启动拓扑发现的过程,DI 为 1B,用于存储节点 i 本身的 ID。

(2) ISF(TI=2)。传感器节点 j 发送 ISF 给拓扑发现的簇头节点,DI 为 1B,用于存储节点 j 的 ID。

(3) TSF(TI=3)。拓扑发现过程的簇头节点将它所建立的调度表通过 TSF 发给传感器节点,DI 为多字节,第 1 个字节表示 DI 总字节数,其余字节为每个节点 ID 和分配相应时隙的调度表。

选举帧用于进行簇内最小剩余能量节点的选举,包括选举请求帧(Request to Vote, RTV)、选举发送帧(Send to Vote, STV)、选举获胜帧(Victorious Vote Frame, VVF)和选举失败帧(Failing Vote Frame, FVF)。

(1) RTV(TI=4)。节点 i 发送 RTV 给它的簇头节点来发起选举过程,DI 为 3B,表示节点 i 本身的剩余能量。

(2) STV(TI=5)。节点 j 发送 STV 给簇头节点,DI 为 1B,表示赞成或反对。

(3) VVF(TI=6)。选举过程的簇头节点发送 VVF 给簇内传感器节点,宣告发起节点 i 在这次选举中获胜,DI 包括 3B,表示节点 i 的剩余能量。

(4) FVF(TI=7)。选举过程的簇头节点发送 FVF 给簇内传感器节点,宣告发起节点 i 在这次选举中失败,DI 包括 3B,表示节点 i 的剩余能量。

2. 时隙划分的能量有效性原则

(1)每个节点都分配有上行时隙和下行时隙,不需要竞争机制。

(2)簇内同一时刻只有一个传感器节点发送数据给簇头节点,簇头之间同一时刻只有一个节点发送数据给 Sink 节点,避免了由于冲突引起的数据帧丢失。

(3)不需要额外的控制帧。

(4)在属于自己的时隙内,帧发送完毕,监听一段时间后,节点进入休眠态。

(5)依据局部时序原则,在时间基准未到达之前,完成数据接收任务的簇头节点进入休眠态,关闭射频模块。

【定义 8.5】设传感器节点的传感器采样频率为 F_S(Hz),传感器信道数量为 s,采样值的大小为 t(bit),数据产生率为 D_S(Kb/s),则封装 D_s 数据帧大小为 D_f,数据帧中除采集数据位数外的其他标识和校验位总数为 D_b。则

$$D_s = F_s \times s \times t \tag{8.3}$$

$$D_f = D_s + D_b \tag{8.4}$$

【定义 8.6】 设 C_t 为固定时间间隔，T_t 为 RTS 结束到 CTS 开始的时间长度，R_t 为 RTS 帧的时间长度，时隙内必要的时间间隔为

$$\mathrm{TA} = 1.5 \times (C_t + T_t + R_t) \tag{8.5}$$

【定义 8.7】 设网络中传感器节点总数为 m_s，信道吞吐量为 $q(\%)$，簇头节点总数为 m_c，节点无线通信速率为 V_c，网络延时为 $t_i(1 \leqslant i \leqslant m_s)$，控制帧帧数为 f_k，最大控制帧的位数为 D_k，则所有传感器节点发送一次采样数据给簇头节点的总时间 t_1 为

$$t_1 = \frac{(F_s \times s \times t + D_b + f_k \times D_k) \times (m_s + 1)}{V_c} + \sum_1^{m_s} t_i + \mathrm{TA} \tag{8.6}$$

所有传感器节点时隙大小相等，时隙大小分配依据下式：

$$t_{\mathrm{ssx}} = \frac{(F_s \times s \times t + D_b + f_k \times D_k) \times (m_s + 1)}{m_s \times V_c} \tag{8.7}$$

无线传感器网络内所有簇头节点发送聚集数据给 Sink 节点的总时间（包括通过多跳与 Sink 节点通信的簇头节点）为

$$t_2 = \frac{(F_s \times s \times t + D_b + f_k \times D_k) \times (m_c + 1) \times (m_s + 1)}{q \times V_c} + \sum_1^{m_c} t_j + \mathrm{TA} \tag{8.8}$$

所有簇头节点时隙大小互不相等，时隙大小分配依据下式：

$$t_{\mathrm{csx}i} = \frac{(F_s \times s \times t + D_b + f_k \times D_k) \times (m_c + 1) \times (m_s + 1)}{q \times V_c} \times \frac{m_i}{m_s} \quad (i = 1, 2, \cdots, m_c) \tag{8.9}$$

控制帧在时隙中的时间宽度 t_k 为数据帧的 1/2，即

$$t_k = \frac{(F_s \times s \times t + D_b)}{2V_c} \tag{8.10}$$

网络初始化阶段，每个簇头节点将各自簇内传感器节点的数量值代入式(8.6)、式(8.9)，则 2 层网络时隙分配的大小便可确定，从而数据传输一个回合的时间也基本确定。对于智能监测的无线传感器网络，主要是完成周期性的数据采集和突发事件报警两大主要功能，因此数据采集频率设置较低，数据产生率不大，依据式(8.6)~式(8.10)进行非均匀时隙的划分，簇内传感器节点时隙宽度较小，簇头时隙宽度较大，且簇头时隙宽度互不相等。簇内每个传感器节点在簇头节点分配的时隙里，一次传送一组大小预先设定好的数据，数据恒速传送。传感器节点在自己的时隙内发送完数据后，监听一段时间，无线通信模块由工作模式切换到掉电模式，进入休眠状态。

图 8.13 为网络节点使用 ASVMAC 算法传输数据的时序图。其中，TX 表示数据发送，RX 表示数据接收，T_s 为传感器节点发送数据时隙，T_m 为节点监听信道时间，T_c 为簇头节点发送数据时隙，T_1 为传感器节点通信时隙重复周期，T_2 为簇头节点通信时隙重复周期，T_3 为平均重复周期（一个时间帧）。每个时隙完成同步序列、控制帧、数据帧和上行链路中防止时隙重叠的时间保护间隔序列。

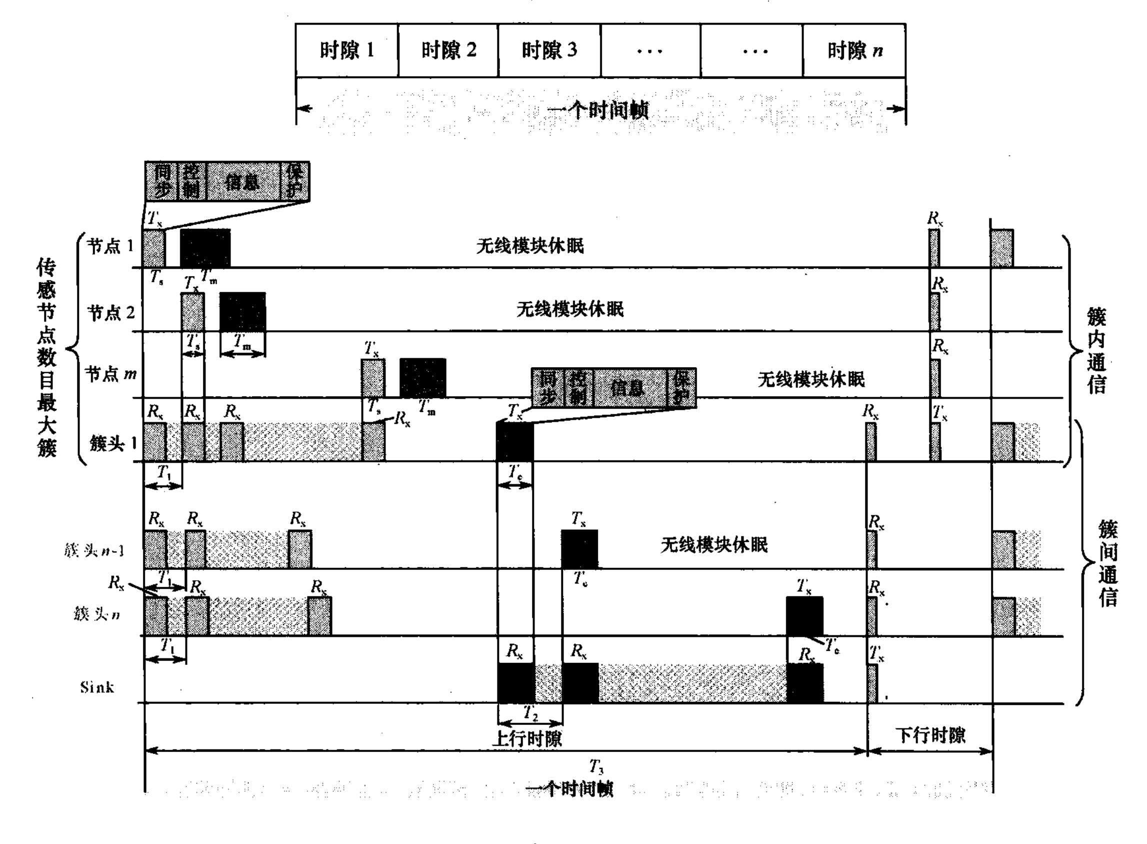


图 8.13　ASVMAC 算法数据传输时隙分配示意图

3. TDMA 调度表初始化

TDMA 调度表初始化在路由发现和簇形成过程中进行。首先，由簇头节点划分簇，划入各簇内的传感器节点上报自己的 ID 号；其次，簇头节点上报各自的成簇信息，由 Sink 节点确认簇头节点和各个簇内传感器节点的数量，根据 ID 号的多少分配簇内时隙数量；最后，依据局部时序原则及系统时钟确定的回合时间不等分簇头时隙，并确定时间基准。由于初始状态下，节点还没有调度表，无法按照调度表来轮流发送数据，因此，当调度表初始化完成后，节点就可以根据调度表进行正常通信。

4. 选举算法

ASVMAC 协议将时间帧分为 4 个阶段：

(1)数据传输阶段。节点周期采集数据，在各自时隙内将数据路由到 Sink 节点。

(2)选举阶段。初始状态下，由于所有节点剩余能量都相同，每个节点都存有调度表和休眠节点的剩余能量 W_e，以便定期与自己的剩余能量比较，一旦发现自己剩余能量低于 W_e，就给簇头节点发送 RTV 来发起一次选举过程，只有当所有邻居节点的剩余能量都高于选举发起节点的能量时，该节点才成为休眠节点。在选举过程，簇头节点广播 RTV 给传感器节点，传感器节点回馈 STV，从而选举出新的休眠节点。选举过程集成在数据传输过程中，控制帧与数据帧一起发送。在选举过程中，选举的发起节点 i 的操作算法和邻节点 j 在节点所发起的选举中的操作见表 8.2。在同一时间，可能会有多个节点同时发起选举，如果这种情况发生，就将剩余能量最少的节点选举为休眠节点。

(3)选举引起的重组阶段,紧跟在一个选举阶段之后,如果发现有节点失效或新节点加入,Sink节点根据表8.3对调度表(簇内节点时隙)进行重新分配。

(4)事件触发的重组阶段,节点能量小于特定值,网络拓扑发生变化等事件触发Sink节点重新分配时隙。

表8.2 选举操作流程

选举请求	选举发送
if 传感器节点 i 的能量 < 休眠节点的能量 then 发送 RTV end if if 节点 i 收到所有邻居节点 STV 且 DI 为赞成 then 更新调度表,簇头节点发送 VVF else if 节点 i 收到所有邻居节点 STV, DI 为反对 then 簇头节点发送 FVF else if 节点未收到所有邻节点 STV then 节点 i 发送 IRF 开始拓扑发现 end if	if 节点 j 的能量 > 发送节点 i 的能量 then 节点 j 发送 STV, DI 为赞成 else 节点 j 发送 STV 且 DI 为反对 end if if 节点 j 收到节点 i 的 VVF then 更新调度表 else if 节点 j 接收节点 i 的 FVF then 节点 j 检测自己的剩余能量并决定是否进入选举 end if

表8.3 调度表初始化和重建流程

初始化	重新创建
传感器节点根据自己的 ID 号等待一段时间 if 未收到 IRF then 继续等待 end if if 接收到 IRF then 发送 ISF end if if 接收到 ISF 且等待足够长的时间 then 根据 ID 号创建调度表, 发送 TSF end if 发送 ISF	if 传感器节点失效 or 新节点加入 then 簇头发送 IRF, 等待 ISF end if if 接收到 IRF then 发送 ISF end if if 接收到 ISF 且等待足够长的时间 then 根据 ID 号创建调度表 end if 发送 ISF

5. 低功耗动态管理协议

簇内每个传感器节点都使用能源控制协议,传感器节点采集数据时,关闭无线收发模块,通过设置合适的占空比,在属于自己的时隙中,打开发送装置,进行数据传输。元数据比采集数据小得多,在智能监测设计中,元数据大小只有采集数据的1/20,传输元数据只需耗费很少的能量,因此元数据传输完毕,不必监听信道直接进入休眠模式。

8.4.4 ASVMAC协议能耗有效性分析

1. 参数设置

通过对ASVMAC、DE-MAC和简单的TDMA协议进行仿真比较,以验证本文ASV-MAC协议算法的能量有效性。依据本文网络的特点,仿真参数如下:传感器节点数为100个,簇头节点数为10个,在不影响协议算法性能的前提下,简化仿真难度,设其中5个簇

内分别有 7 个传感器节点，另外 5 个簇内有 11 个传感器节点，簇头节点通信时隙分别为 20ms 和 30ms，传感器节点时隙大小为 5ms，监听时间 5ms，每个传感器节点产生等量数据，每个节点每隔 300ms 产生一帧数据需要发送到 Sink 节点，仿真时间分别为 500s 和 10000s，每个节点的初始能量为 10J。

2. 性能分析

在仿真开始后，ASVMAC 先初始化 TDMA 调度表，之后每隔一个时间帧周期通过选举更新调度表，每个节点的操作，根据能量模型进行能耗记录：

（1）平均能耗比较。从图 8.14 中可以看出，虽然能耗随时间变化基本均匀，但由于 ASVMAC 采用了簇内最低能量节点的选举机制，因此网络能量得到有效均衡，网络整体能量消耗较慢。

（2）随着仿真时间的增加，3 种协议平均能耗均有不同程度的上升，但由于 ASVMAC 协议能够减少空闲侦听，避免信道冲突，加之选举机制的作用，其能耗速度增加较为缓慢，如图 8.15 所示。体现了较好的协议性能，有效延长网络的使用寿命。

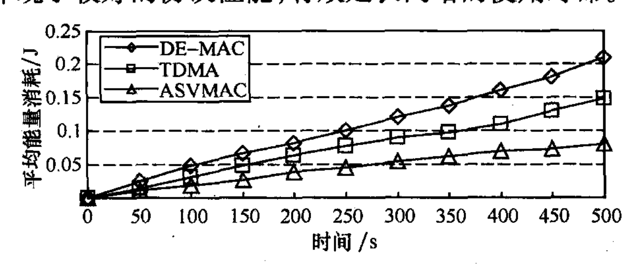


图 8.14　500ms 时间内的平均能耗比较

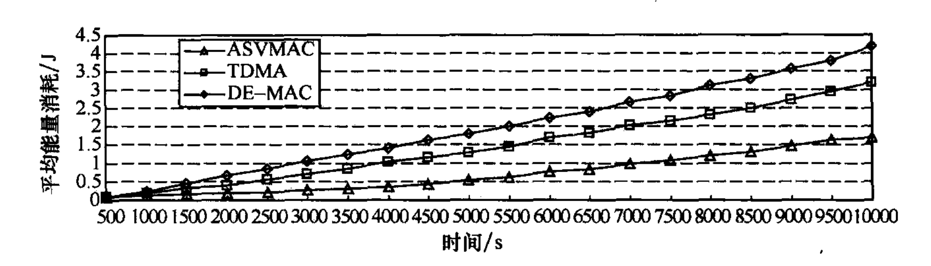


图 8.15　10000ms 时间内的平均能耗比较

参 考 文 献

[1] Akyildiz I, Su W, Sankarasubramaniam Y, etc. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38 (4): 393 -422.

[2] Tanenbaum A S. Computer Networks[M]. Prentice - Hall, Englewood Cliffs, NJ, third edition, 1997.

[3] Demirkol I, Ersoy C, Alagoz F. MAC Protocol for wireless Sensor Networks: A Survey[J]. IEEE Communications Magazine, April 2006: 115 - 121.

[4] Kredo K, Mohapatra P. Medium Access Control in Wireless Sensor Networks[J]. Computer Netwoks, 2007, (51): 961 -994.

[5] Singh S, Raghavendra C. PAMAS - Power Aware Multi - Access Protocol with Signaling for Ad hoc Networks[J]. SIG-

COMM Computer Communications Review, 1998,3(28):5 -26.

[6] Ye W, Heidemann J, Estrin D. Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks [J]. IEEE/ACM Trans. On Networking, 2004,12(3):493 -505.

[7] Lin P, Qiao C, Wang X. Medium Access Control with a Dynamic Duty Cycle for Sensor Networks[C]. Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC), 2004, 3:1534 -1539.

[8] Dam T V, Langendoen K. An Adaptive Energy - Efficient MAC Protocol for Wireless Sensor Networks[C]. Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys'03), November, 2003, Los Angeles.

[9] 龚海刚, 刘明, 王晓敏. TLTS: 大规模无线传感器网络下基于簇的两级 TDMA 调度协议[J], 计算机研究与发展, 2007, 44(1):71 -77.

[10] Polastre J, Hill J, Culler D. Versatile Low Power Media Access for Wireless Sensor Networks[C]. Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys'04), Baltimore. November, 2004.

[11] El - Hoiydi A, Decotignie J D. WiseMAC: An Ultra Low Power MAC Protocol for the Downlink of Infrastructure Wireless Sensor Networks[C]. Proceedings of the Ninth IEEE Symposium on Computers and Communications(ISCC'04), Alexandria. June, 2004.

[12] Rajendran V, Obraczka K, Garcia J J. Energy - Efficient, Collision - Free Medium Access Control for Wireless Sensor Netwoks[C]. Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys'03), November, 2003, Los Angeles.

[13] IEEE. IEEE Standard 802. 15. 4: Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for Low - Rate Wireless Personal Area Networks, 2003.

[14] Rhee I, Warrier A, Aia M, etc. Z-MAC: a Hybrid MAC for Wireless Sensor Networks[J]. Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys'05), San Diego. November, 2005.

[15] Waharte S, Boutaba R. Performance Comparison of Distributed Frequency Assignment Algorithms for Wireless Sensor Networks[C]. Proceedings of the IFIP International Conference on Network Control, Los Alamitos, 2004:217 -228.

[16] Wireless Sensor Networks Product Reference Guide[M]. Crossbow Company, USA, 2007.

[17] Hui Lin X, Kwong Kwok Y. On Channel Adaptive Energy Management in Wireless Sensor Networks[C]. Proceedings of the International Conference on Parallel Processing(ICPP) 2005, June, 2005:397 -404.

[18] Ho S B, Su X. CuMPE: Cluster - Management and Power - Efficient Protocol for Wireless Sensor Networks[C]. Information Technology: Research and Education, 2005. ITRE 2005. 3rd International Conference on, June 2005: 60 -67.

[19] cmclab [EB/OL]. http://www - ece. rice. edu/ ~ cavallar/,2003,12.

第9章　无线传感器网络路由协议

无线传感器网络路由协议是保证无线传感器网络高效通信的另一关键网络协议。网络层路由协议以数据为中心，控制网络的运作、负责路由数据帧、完成流量控制功能。网络层有两个相互关联的问题：一是各节点采用自组织的方式构建网络，并确定网络拓扑结构；二是在给定的网络拓扑结构下，如何进行路由。拓扑控制协议负责拓扑结构的建立和维护，路由协议负责将传感节点采集的数据转发至Sink节点。网络中支持数据传输的路由协议必须能感知拓扑结构的变化，并随之调整路由路径。

在无线传感器网络中，路由协议不仅关心单个节点的能量消耗，更关心整个网络能量的均衡消耗，这样才能延长整个网络的生存期。同时，无线传感器网络是以数据为中心的，这在路由协议中表现得最为突出，每个节点没有必要采用全网统一的编址，选择路径可以不用根据节点的编址，更多的是根据感兴趣的数据建立数据源到汇聚节点之间的转发路径。

9.1　路由协议概述

无线传感器网络路由协议主要包括两方面的功能：寻找源节点和目的节点之间兼顾总能耗、延时、能耗均衡性等指标的优化路径；将感知数据沿着优化路径正确转发。路由算法在路由协议中起到至关重要的作用，采用何种算法往往决定了最后的路径搜索结果。通常需要综合考虑以下几个设计指标：

(1)最优化。指路由算法选择最佳路径的能力。

(2)简洁性。算法设计简洁，利用最少的软件和开销，提供最有效的功能。

(3)鲁棒性。路由算法处于非正常或不可预料的环境时，如硬件故障、负载过高或操作失误时，都能正确运行。由于路由器分布在网络连节点上，所以它们出故障时会产生严重后果。最好的路由算法通常能经受时间的考验，并在各种网络环境可靠工作。

(4)快速收敛。收敛是在最佳路径判断上所有路由器达到一致的过程。当某个网络事件引起路由可用或不可用时，路由器就发出更新信息。路由更新信息遍及整个网络，引起重新计算最佳路径，最终达到所有路由器一致公认的最佳路径。收敛慢的路由算法会造成路径循环或网络中断。

(5)灵活性。路由算法可以快速、准确地适应各种网络环境。例如，某个网段发生故障，路由算法要能很快发现故障，并为使用该网段的所有路由选择另一条最佳路径。

由于无线传感器网络有不同于传统无线网络的特点，如资源有限、规模更大、节点没有一个全局性的标识、能量有限和采取数据为中心的路由方式等，因此，路由问题是无线传感器网络的一个非常重要的问题，网络的路由协议的设计非常具有挑战性。

在无线传感器网络中,路由协议负责将数据包从源节点通过中继节点转发到目的节点或用户。无线传感器网络中数据路由的研究分为两类:一是针对同构的传感器节点相互协作,进行数据收集、处理和路由,完成传感任务。二是主要针对异构无线传感器网中描述异构的节点、链路的状态信息的研究。目前,异构网络是无线传感器网络路由协议研究的重点。

由于整个网络中可能存在大量的传感器节点,对应着大量的资源状态信息,要将所有节点、链路的所有信息完整、及时地发送到每个节点是不现实的。在网络中发送洪泛信息将消耗大量的能源,甚至可能造成网络的拥塞,使异构无线传感器网络无法完成传感数据的传送。因此,研究高效、动态地汇聚、分发和更新网络资源状态信息的协议对异构无线传感器网络是非常重要的。

很多传感应用中对传感数据的路由有服务质量要求,例如,监测环境温度的无线传感器网络,必须将感知到的异常的温度数据,如火灾发生时,及时传送到观察者。如果不能及时传送到,观察者和决策系统就无法做出及时的响应,传感数据就失去了采集的意义。在同构的无线传感器网络中,在为有传输时延限制的传感数据寻找路由时,通常只需考虑通信链路的时延。在异构的无线传感器网络中,在选择路由时,还必须将潜在的通路中各个节点的不同通信能力、通信愿望以及通信链路的质量等因素纳入考虑范围。因此,需要研究异构无线传感器网络中支持服务质量的数据路由算法。

在无线传感器网络中,传感器节点经常由于环境的变化或电源耗尽而失效。同时,由于传感器节点的通信能力有限,而无线传感器网络又常常部署在恶劣的环境中,传感器节点之间的通信容易受各种自然因素的影响而导致失败。这些都会导致网络拓扑的变化。异构传感器网络的信息是海量的,这些信息来源于异构动态变化的网络,存在大量的冗余数据和不可靠的数据,研究鲁棒路由算法,对支持传感数据被可靠、正确地转发到基站节点是非常必要的。在异构无线传感器网络中,不同的传感器节点可能具有不同的通信愿望和通信能力,这使得可靠、正确地发送传感数据变得更为困难。特别地,当缺乏网络状态信息时,异构无线传感器网络需要鲁棒性很强的路由算法来保证数据的可靠发送。

9.2　路由协议分类

由于无线传感器网络与应用高度相关,单一的路由协议难以满足各种应用需求。关于网络层的路由方式,根据采用的划分与评价标准的不同有多种分类。可依据路由协议采用的通信模式、路由结构、路由建立时机、状态维护、节点标识和投递方式等策略,对目前提出的路由协议进行分类。

根据传输过程中采用路径的多少,可分为单路径路由协议和多路径路由协议。单路径路由节约存储空间,数据通信量少。多路径路由容错性强、健壮性好,且可从众多路由中选择一条最优路由。

根据节点在路由过程中是否有层次结构、作用是否有差异,可分为平面路由协议和层次路由协议。平面路由简单、健壮性好,但建立、维护路由的开销大,数据传输跳数多,适合小规模网络。层次路由扩展性好,适合大规模网络,但簇的维护开销大且簇头是路由的关键节点,其失效将导致路由失败。

根据路由建立时机与数据发送的关系，可分为主动路由协议、按需路由协议和混合路由协议。主动路由建立、维护路由的开销大，资源要求高；按需路由在传输前需计算路由，时延大；混合路由则综合利用这两种方式。

根据是否以地理位置来标识目的地、路由计算中是否利用地理位置信息，可分为基于位置的路由协议和非基于位置的路由协议。有大量无线传感器网络应用需要知道突发事件的地理位置，这是基于位置的路由协议的应用基础，但需要 GPS 定位系统或其他定位方法协助节点计算位置信息。

根据是否以数据来标识目的地，可分为基于数据的路由协议和非基于数据的路由协议。有大量 WSNs 应用要求查询或上报具有某种类型的数据，这是基于数据的路由协议的应用基础，但需要分类机制对数据类型进行命名。

根据节点是否编址、是否以地址标识目的地，可分为基于地址的路由协议和非基于地址的路由协议。基于地址的路由在传统路由协议中较常见，而在无线传感器网络中一般不单独使用，而与其他策略结合使用。

根据路由选择是否考虑 QoS 约束，可分为保证 QoS 的路由协议和不保证 QoS 的路由协议。保证 QoS 的路由协议是指在路由建立时，考虑时延、丢包率等 QoS 参数，从众多可行路由中选择一条最适合 QoS 应用要求的路由。

根据数据在传输过程中是否进行聚合处理，可分为数据聚合的路由协议和非数据聚合的路由协议。数据聚合能减少通信量，但需要时间同步技术的支持，并使传输时延增加。

根据路由是否由源节点指定，可分为源站路由协议和非源站路由协议。源站路由协议节点无需建立、维护路由信息，从而节约存储空间，减少通信开销。但如果网络规模较大，数据包头的路由信息开销也大，而且如果网络拓扑变化频繁将导致路由失败。

根据路由建立时机是否与查询有关，可分为查询驱动的路由协议和非查询驱动的路由协议。查询驱动的路由协议能够节约节点存储空间，但数据时延较大，且不适合环境监测等需紧急上报的应用。

此外，文献[1]从网络结构和路由协议运行机制两个方面对路由协议进行分类，结果如图 9.1 所示。

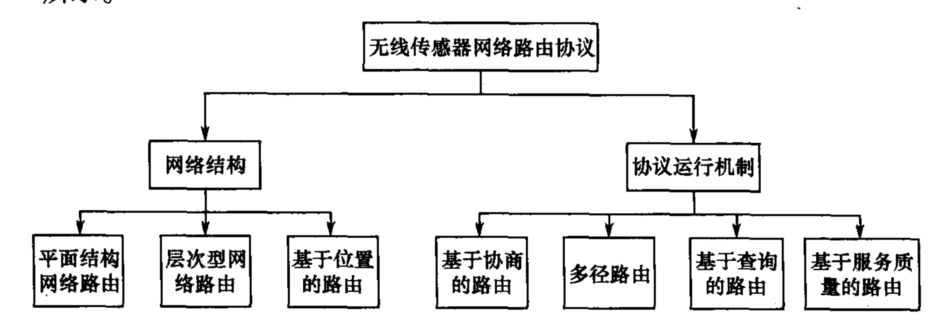


图 9.1　路由协议分类

本章的相关研究主要根据网络结构划分的平面路由与分层路由方式展开研究。在平面路由中，所有的节点具有相同的地位和功能，节点间协同工作共同完成感知任务。与无线自组织网络不同的是，由于无线传感器网络内的节点分布密度更大，网络内相邻节点间

数据的采集又大都基于同一现象,因此,每个节点不但没有全局唯一的标识而且网内传输的数据会出现冗余。这种情况促成了构建以数据为中心的平面路由协议,数据通过基于属性的命名机制难以描述。中间节点在传输数据过程中对数据进行融合以降低节点能耗。分层型路由的基本思想是将传感器网络分解为相互连接的簇,簇内节点只和本簇的簇头通信,簇头节点先进行数据聚集,减少冗余信息传输量,再把聚集的数据传送给终端节点。这种方式能满足传感器网络的可扩展性,有效的维持传感节点的能量消耗,延长网络生命周期,从而保证任务的可持续性。

9.3 路由协议研究现状

就无线传感器网络的应用场合以及传感节点与Sink节点间的数据传输模式而言,可将无线传感器网络分为连续监测、事件驱动和用户查询3种类型。迄今为止,针对3种应用类型的路由协议研究已有很多。

9.3.1 典型路由协议原理

1. 以数据为中心的路由算法

以数据为中心的路由算法的代表有泛洪(Flooding)[2]、SPIN[3]和定向扩散[4]等路由算法。

利用泛洪路由算法进行节点间信息传递时,每个节点将接收到的数据包,连同自身的感知数据,发送至所有的邻节点,重复执行此过程,直到数据包被发至Sink或达到预先设定的最大跳数为止。泛洪路由的优点在于实现起来简单,但易引起内爆、重叠和资源盲点等问题,如图9.2和图9.3所示。

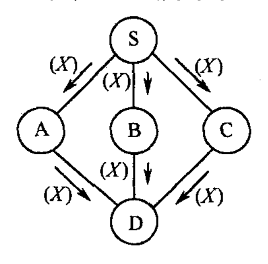


图9.2 泛洪的内爆问题

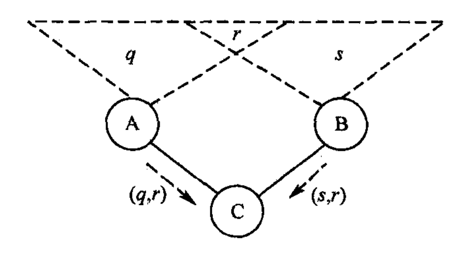


图9.3 泛洪的消息重叠问题

SPIN路由的特点在于节点间的协商机制。节点在将信息传递给邻节点前,先向邻节点发送广播信息,邻节点根据广播信息判断待传递的信息是否是自身感兴趣的,如若感兴趣,则发出请求,等待接收信息。SPIN路由可有效解决泛洪路由的缺点,并且可根据具体应用灵活地设置广播信息的格式,以减少由于广播信息而引起的能耗。SPIN路由的最大缺点在于广播—应答机制只适用于相邻节点,即单跳节点,而不能保证多跳时信息的有效传输。对于图9.4所示的网络中,节点C对节点A的信息感兴趣,节点A需经节点B才能将信息传输至节点C,但节点B并不对节点A的信息感兴趣,导致信息无法传输至节点B。这一缺点使得SPIN路由无法用于需要在节点间多跳可靠地传输信息的场合,如冲突监测。

定向扩散算法的主要思想是对网络中的数据用一组属性对命名,基于数据进行通信,采用查询驱动数据传送模式。当 Sink 节点对某事件发出查询命令时就开始一个新的定向扩散过程,它由查询扩散,初始梯度建立和数据传送 3 个阶段构成,如图 9.5 所示。在路由过程中,所有的通信都是在相邻节点间进行的,无需在节点间使用地址标识节点。

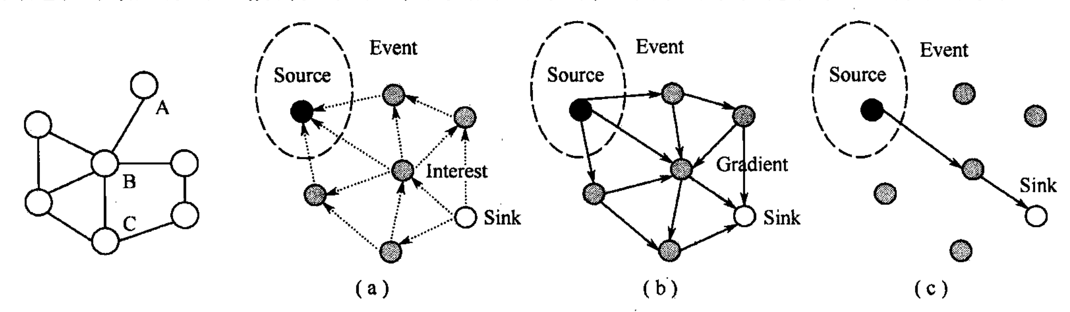


图 9.4　SPIN 路由无法保证多跳可靠传输示意图

图 9.5　定向扩散路由过程

不过,定向扩散的数据传递模式属于查询型,使得其无法用于需连续传输感知信息的场合。此外,定向扩散路由所使用的属性对命名机制需预先定义,且与应用相关。同时,感知信息和查询信息的匹配也要消耗额外的能量。

2. 基于位置信息的路由算法

基于位置信息的代表性路由算法有 MECN[5]、GAF[6]、GEAR[7]和 GPSR 协议[8]等。

这类路由的缺点是依赖节点的 GPS 定位信息,成本较高。给每个节点加装 GPS 会消耗节点的能量,也会增大节点的体积。

MECN 协议为每个节点设置了转发区域,转发区域可以表示为一组节点集,发送节点通过转发区域内的节点发送数据,与直接将数据传递到目的节点相比,这种方式需要能量较少。节点对(i, r)的转发区域如图 9.6 所示。那么节点 i 到达的目的节点所产生的所有转发区域的集合,就构成了节点 i 的外围。

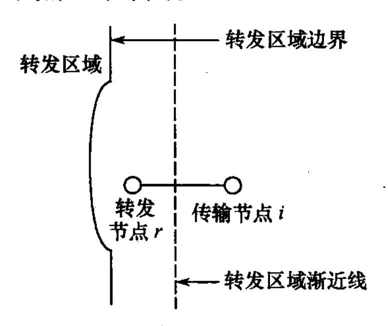


图 9.6　MECN 协议传输—转发节点对的转发区域

MECN 的主要设计思想是构建子网,要求子网内部所含节点的数目较少并且任意两个节点间传输数据都消耗更少的能量。这样,不必考虑网络内所有的节点,就可以发现全局最小能量的路径。这对每个考虑到自身转发区域的节点来说,利用本地搜索就可以实现到达目的节点的最小能量路径。

MECN 的运行分为位置获取和路径搜索两个阶段:第一阶段是获取二维平面的位置信息,并构建包含所有发送节点外围的外围图。外围图的构建由节点内部的本地计算来完成。第二阶段是在外围图中搜索最优链路,搜索过程采用以能耗为代价度量的分布式 Bellman-Ford 最短路径算法来实现。

MECN 协议具有自动重配置的特点,因此可以动态地适应节点的失效和网络分布。但 MECN 协议是在假定网络内每两个节点都能直接通信,即网络是在充分连接的前提下提出的,这在实际环境中并不容易做到。尽管 MECN 协议最初是为无线自组织网络设计的,但该协议同样适用于节点固定或少量节点移动的无线传感器网络。

GAF 算法是以节点的地理位置为依据的分簇算法,该算法把监测区域划分成虚拟单元格,将节点按照位置信息划入相应的单元格;在每个单元格中定期选举产生一个簇头,只有簇头保持活动,其他节点进入休眠状态。GAF 算法的执行也包括两个阶段:第一阶段是虚拟单元格的划分,根据节点的位置信息和通信半径,将网络区域划分成若干虚拟单元格,保证相邻单元格中的任意两个节点能够直接通信;第二阶段是虚拟单元格中簇头节点的选择。节点周期性地进入休眠和工作状态,从休眠状态被唤醒之后与本单元格内其他节点交换信息,以确定自己是否需要成为簇头。每个节点可处于发现、活动及休眠 3 种状态。

在网络初始化时,所有节点都处于发现状态,每个节点都通过发送消息通告自己的位置、ID 等信息,经过此阶段,节点能得知同一个单元格中其他节点的信息。然后,每个节点将自身定时器设置为某个区间内的随机值,一旦定时器超时,节点发送消息声明它进入活动状态,成为簇头。节点如果在定时器超时之前收到来自同一单元格内其他节点成为簇头的声明,说明它自己这次簇头竞争失败,进入休眠状态。

GEAR 是充分考虑了能源有效性的基于位置的路由协议,它比其他的基于位置的路由协议能更好地应用于无线传感器网络之中。

GEAR 算法提出,既然传感器网络中的数据经常包含了位置属性信息,那么可以利用这一信息,把在整个网络中扩散的信息传送到适当的位置区域中。同样,GEAR 也采用了查询驱动数据传送模式。它传送数据分组到目标域中所有的节点的过程包括两个阶段:目标域数据传送和域内数据传送。

在目标域数据传送阶段,当节点接收到数据分组,它将邻节点同目标域的距离和它自己与目标域的距离相比较,若存在更小距离,则选择最小距离的邻节点作为下一跳节点;若不存在更小距离,则认为存在“hole”,节点将根据邻居的最小花销来选择下一跳节点。

在域内数据传送阶段,可通过两种方式让数据在域内扩散:在域内直接洪泛和递归的目标域数据传送直到目标域剩下唯一的节点,如图 9.7 所示。

GEAR 将网络中扩散的信息局限到适当的位置区域中,减少了中间节点的数量,降低了路由建立和数据传送的能源开销,从而更有效地提高了网络的生命周期。缺点是依赖节点的 GPS 定位信息,成本较高。

如果 Sink 节点的一次查询只需一次上报,Directed Diffusion 协议开销就太大了,Rumor 协议[9]正是为解决此问题而设计的。该协议借鉴了欧氏平面图上任意两条曲线交叉几率很大的思想。当节点监测到事件后将其保存,并创建称为 Agent 的生命周期较长的包括事件和源节点信息的数据包,将其按一条或多条随机路径在网络中转发。收到 Agent

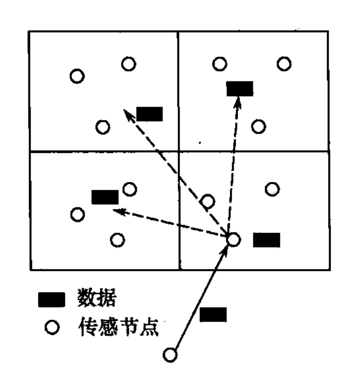


图9.7　GEAR中递推的目标域数据传送

的节点根据事件和源节点信息建立反向路径，并将Agent再次随机发送到相邻节点，并可在再次发送前在Agent中增加其已知的事件信息。Sink节点的查询请求也沿着一条随机路径转发，当两路径交叉时则路由建立；如不交叉，Sink节点可泛洪查询请求。在多Sink点、查询请求数目很大、网络事件很少的情况下，Rumor协议较为有效。但如果事件非常多，维护事件表和收发Agent带来的开销会很大。图9.8表示了Rumor协议中Agent传播和Agent路径与查询路径的交叉情形。

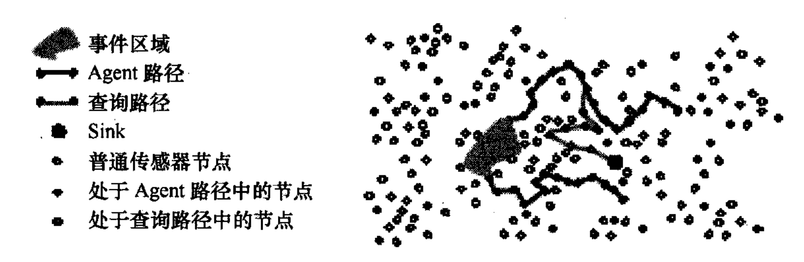


图9.8　Rumor协议中Agent传播和Agent路径与查询路径的交叉

GPSR协议[10]也是一个典型的基于位置的路由协议。使用GPSR协议，网络节点都知道自身地理位置并被统一编址，各节点利用贪心算法尽量沿直线转发数据。产生或收到数据的节点向以欧氏距离计算最靠近目的节点的邻节点转发数据，但由于数据会到达没有比该节点更接近目的点的区域（称为空洞），导致数据无法传输，当出现这种情况时，空洞周围的节点能够探测到，并利用右手法则沿空洞周围传输来解决此问题。该协议避免了在节点中建立、维护、存储路由表，只依赖直接邻节点进行路由选择，几乎是一个无状态的协议。且使用接近于最短欧氏距离的路由，数据传输时延小，并能保证只要网络连通性不被破坏，一定能够发现可达路由。其不足是当网络中Sink节点和源节点分别集中在两个区域时，由于通信量不平衡易导致部分节点失效，从而破坏网络连通性，需要GPS定位系统或其他定位方法协助计算节点位置信息。

TBF协议[11]是一个基于源站和基于位置的路由协议。与GPSR协议不同，TBF协议不是沿着最短路径传播；与通常的源站路由协议不同，TBF协议利用参数在数据包头中指定了一条连续的传输轨道而不是路由节点序列。网络节点利用贪心算法根据轨道参数和邻节点位置，计算出最接近轨道的邻节点作为下一跳节点。该协议可利用GPSR协议的

方法或其他方法避开空洞；通过指定不同的轨道参数，很容易实现多路径传播、广播、对特定区域的广播和多播；源站路由避免了中间节点存储大量路由信息；指定轨道而不是节点序列，数据包头的路由信息开销不会随着网络变大而增加，允许网络拓扑变化，避免了传统源站路由协议的缺点。但随着网络规模变大，路径加长，沿途节点进行计算的开销也相应增加；且需要 GPS 定位系统或其他定位方法协助计算节点位置信息。图 9.9 表示使用 TBF 协议沿着任意曲线传输数据。

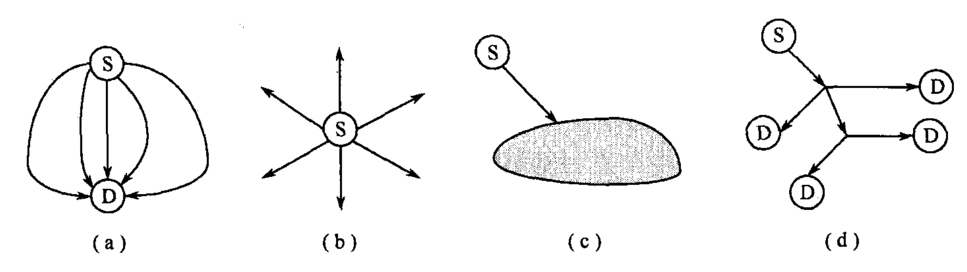


图 9.9　TBF 协议沿着任意曲线传输数据

(a)多路径传播；(b)广播；(c)对特定区域广播；(d)多播。

3. 分层型路由

分层型路由的主要代表有 LEACH[9]、PEGASIS[8] 和 TEEN[10] 等。其基本原理如图 9.10 所示。

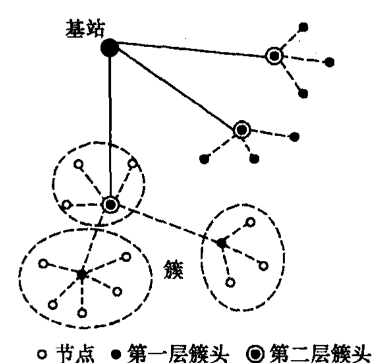


图 9.10　分层型路由的基本原理

Heinzelman 等人在文献[9]中给出了一种基于概率的低功耗自适应分簇协议（Low Energy Adaptive Clustering Hierarchy，LEACH），同时给出了簇头产生算法。LEACH 路由最大的优势在于它是一种完全分布式的路由，无需网络的全局信息。

对于节点 n，产生 0 ~ 1 之间的随机数，与阈值 $T(n)$ 比较，若该随机数小于 $T(n)$，则节点 n 在当前轮成为簇头。阈值 $T(n)$ 的计算公式如下：

$$T(n) = \begin{cases} \dfrac{p}{1 - p[r \bmod (1/p)]} & (n \in G) \\ 0 & (n \notin G) \end{cases} \tag{9.1}$$

式中：p 为簇头比例；r 为当前轮数；G 为候选簇头集（前 $r-1$ 轮内未担任过簇头的节点集）。

LEACH 协议可保证每个节点在一个监测周期内有且仅有一次机会成为簇头，从而避免部分节点长期担任簇头引起的能耗不均衡问题。但由于 LEACH 单纯以概率的方式产生簇头，未考虑节点之间的距离，会出现相邻簇头距离很近的现象。此外，已有研究表明 LEACH 还存在以下几个问题[10]：

(1)产生的簇头数目与总能耗最小时的最优簇数目不一致，只有在不到 20% 的情况下两者相吻合。

(2)未考虑能量对节点地位的影响，剩余能量低的节点也可能被选为簇头，会加速这些节点的死亡。

(3)节点在每一轮都需要产生随机数并计算阈值 $T(n)$，需要消耗一定的计算资源。

PEGASIS 路由算法的思想是将节点以链的形式组织起来，链上的节点只和最邻近的节点通信，在每条链中选择一个节点和基站通信。研究表明，针对不同的网络规模和拓扑结构，PEGASIS 的性能优于 LEACH。PEGASIS 采用多跳通信可减轻节点的载荷，但对于距离簇头较远的节点，易导致感知信息的延迟。同时，PEGASIS 算法中的簇头是固定的，簇头的能量决定了链的存活期。

TEEN 是一种阈值敏感能量有效的分层型路由算法，特别适用于被监测现象突变的情形。节点形成簇后，簇头向簇内节点广播软、硬两种阈值。当节点的感知数据超过硬阈值，或感知数据的变化量不低于软阈值时，节点才将感知数据传输给簇头，否则其无线发送模块不工作。通过这种方法，可以减少无用信息的传输量。对于需要周期性地向用户报告监测结果的网络，TEEN 则不适用。如果感知数据的变化未达到阈值，用户可能接收不到任何感知数据。

4. 其他协议

Shah 等人提出能量感知路由协议[12]，该协议的目的在于改善 Directed Diffusion 协议的耗能情况，采用地理位置和数据类型(即节点类型)标识节点。Shah 等人认为该协议是按需路由协议，但其含义更多的是查询驱动的，可将其与 Directed Diffusion 都列为主动路由协议。Sink 点(Cost(Sink) = 0)利用受控的泛洪发起建立路由请求，与 Directed Diffusion 相比，该协议虽然存在多条路径，但只选用一条，能够有效节约能源 40% 以上，随机选择路由方式平衡了通信量。其缺点是 Sink 节点需要周期性泛洪维护路由信息，需要进行节点间收发开销和剩余能量测量，根据概率随机选择一条路径导致其可靠性不如 Directed Diffusion 协议。

TTDD 协议[13]是一个层次路由协议，主要是解决网络中存在多 Sink 节点及 Sink 节点移动问题。当多个节点探测到事件发生时，选择一个节点作为发送数据的源节点，源节点以自身作为格状网的一个交叉点构造一个格状网。其过程是源节点先计算出相邻交叉点位置，利用贪心算法请求最接近该位置的节点成为新交叉点，新交叉点继续该过程直至请求过期或到达网络边缘。交叉点保存了事件和源节点信息。进行数据查询时，Sink 节点本地泛洪查询请求到最近的交叉节点，此后查询请求在交叉点间传播，最终源节点收到查询请求，数据反向传送到 Sink 节点。Sink 节点在等待数据时，可继续移动，并采用代理(Agent)机制保证数据可靠传递。与 Directed Diffusion 协议相比，该协议采用单路径，能够提高网络生存时间，但计算与维护格状网的开销较大，节点必须知道自身位置，非 Sink 点位置不能移动，要求节点密度较大。

SAR 协议[14]是第一个在 WSNs 中保证 QoS 的主动路由协议。Sink 点的所有一跳邻节点都以自己为根创建生成树，在创建生成树过程中考虑节点的时延、丢包率等 QoS 参数以及最大数据传输能力，各个节点从而反向建立了到 Sink 点的具有不同 QoS 参数的多条路径。节点发送数据时选择一条或多条路径进行传输。该协议能够提供 QoS 保证，但缺点是节点中的大量冗余路由信息耗费了存储资源，且路由信息维护、节点 QoS 参数与能耗信息的更新均需较大开销。

Chang 等人提出的最大化生存时间路由协议[15]与 Shah 等人的思想有相似之处，认为最小化传输能量并不完全适合无线传感器网络，必须考虑网络的生存时间。它根据节点剩余能量与链路发送数据能量要求定义代价函数，最重要的贡献在于利用网络流建模，采用线性规划方法来解决最大生存时间问题。

TinyOS Beaconing 协议[16]较为简单，首先对节点进行编址，Sink 节点周期性泛洪路由更新消息，信号覆盖范围内的节点接收到更新消息后，将发送消息的节点作为父节点保存到路由表中，然后将该消息在物理信道上广播，从而构成了一个以 Sink 节点为根的广度优先的生成树。这种方式在小规模网络中简单、易用，但在较大网络中将导致节点和 Sink 节点间跳数增加，广播式路由更新消息消耗网络能量，路径建立只与接收到 Beaconing 的时序有关，不进行任何优化，扩展性差。Sink 点周围的节点由于过多地参与数据传输，耗能较多，容易失效。图 9.11 表示了以 Sink 节点 u 为根的生成树的建立过程。

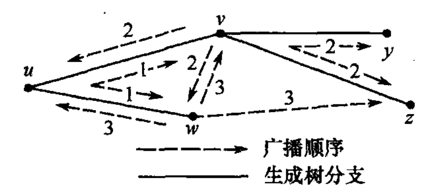


图 9.11 TinyOS Beaconing 协议路由生成树建立过程

Ye 等人提出的最小代价路由协议[13]的思想与很多协议的思想相同，以跳数或能耗作为代价尺度，最终达到最小化代价的目的，其特别之处在于采用退避算法进行代价通告。该协议与 TinyOS Beaconing 相比能节约能量，但仍有一些与其相同的缺点并需测量通信代价。由于代价函数只考虑了能耗最少而没有考虑节点剩余能量，会使通信量分担不平衡，导致某些节点因能量耗尽失效而使网络不能连通。

此外，基于 Agent 的路由，概率型路由，基于蚁群算法的路由和基于模拟退火算法的路由协议陆续被提出来。

9.3.2 路由协议性能比较

由于无线传感器网络具有与应用相关的特点，故无线传感器网络路由协议同样具有多样性的特点，难以进行比较，并且很难说哪个协议更为优越。为便于说明，采用了列表方式，表 9.1 使用本章的分类方法对重点讨论的路由协议进行了分类比较；表 9.2、表 9.3 对这些协议的特点和大致应用范围进行了总结与比较。协议特点包括是否提供最短路径、是否存在由于其失效从而影响路由的关键节点、是否支持 Sink 节点移动、是否支持普通节点移动，以及建立、维护路由的节点所需的通信量、计算量与存储量。应用范围是指协议的较佳使用范围，但不是绝对的，应视具体应用而定。

表 9.1　典型路由协议的分类比较

协 议	分 类						
	Multipath	Unipath	Flat	Hierarchical	Proactive	Reactive	Hybrid
Flooding	√		√		√	√	
Gossiping		√	√		√	√	
SPIN	Possible	Possible	√			√	
Directed Diffusion	√		√		√		
Rumor		√	√				√
GPSR		√	√			√	
TBF	Possible	Possible	√			√	
Shah et al.		√	√			√	
LEACH		√		√		√	
PEGASIS		√		√		√	
TEEN		√		√		√	
TTDD		√		√		√	
SAR	Possible	Possible	√		√		
Chang, et al.		√	√		√		
TinyOS Beaconing		√	√		√		
Ye, et al.		√	√		√		
Flooding	Possible	Possible	Possible				
Gossiping	Possible	Possible	Possible				
SPIN		√			√		√
Directed Diffusion		√		Possible	√		√
Rumor		√			√		√
GPSR	√						
TBF	√					√	
Shah et al.	√	√			√		√
LEACH			√		√		
PEGASIS			√		√		
TEEN			√		√		
TTDD	√	√					
SAR			√	√			
Chang et al.			√				
TinyOS Beaconing			√				
Ye et al.			√				

表9.2　典型路由协议的应用范围比较

协 议	应 用 范 围
Flooding	上报紧急事件、多个 Sink、高传输可靠性、节点频繁移动、节点频繁故障、可扩展性差
Gossiping	多个 Sink、与延迟无关、允许数据丢失、节点移动、可扩展性差
SPIN	多个 Sink、可扩展性差、中层节点知道远处节点是否需要数据
Directed Diffusion	Sink 节点少、查询型应用、对 QoS 有要求、一次性查询周期性响应
Rumor	多个 Sink、事件少、与延迟无关、查询型应用、一次性查询一次性响应、节点密度高
GPSR	基于位置、节点频繁移动、节点密度高
TBF	节点频繁移动、节点密度高、需要多种路由策略
Shah, et al.	知道邻节点传输通信代价、查询型应用
LEACH	对延迟敏感、节点能量高、低扩展性
PEGASIS	对延迟敏感、节点能量高、低扩展性
TEEN	阈值相关
TTDD	多 Sink、Sink 移动、对实时性要求不高、查询型应用
SAR	小规模网络、对 QoS 敏感、可扩展性差
Chang, et al.	节点知道邻节点通信代价、网络存活时间长
TinyOS Beaconing	Small-scale WSNs; low scalability 小规模网络、扩展性差
Ye, et al.	节点知道邻节点通信代价、网络存活时间长、扩展性差

表9.3　典型路由协议的特点比较

协 议	最优路径	关键节点	Sink 移动	普通节点移动	计算开销	通 信 开 销	存储开销
Flooding	最短路径	×	√	√	无需	泛洪数据	无需
Gossiping	×	×	√	√	无需	沿随机路径传输	无需
SPIN	Possible	×	√	√	无需	泛洪 ADV	无需
Directed Diffusion	Possible	×	×	×	计算梯度	泛洪兴趣	存储梯度及缓存兴趣
Rumor	×	×	√	×	联合 Agent	沿随机路径发送查询	存储资源和事件
GPSR	Nearly	×	×	√	计算邻节点至 Sink 节点的距离	获取邻节点位置	无需
TBF	×	×	×	√	计算邻节点至曲线的距离	获取邻节点位置	无需
Shah, et al.	次优	×	×	×	分配邻节点概率	衡量邻节点代价	存储路由表
LEACH	×	簇头	×	×	选举簇头/周期性比较簇头信号强度	周期性分簇	存储簇头

（续）

协 议	最优路径	关键节点	Sink移动	普通节点移动	计算开销	通 信 开 销	存储开销
PEGASIS	×	簇头	×	×	选举簇头	构建链条	存储链条上两个邻节点
TEEN	×	簇头	×	×	选举簇头/周期性比较簇头信号强度	周期性分簇	节点存储簇头信息/簇头存储阈值
TTDD	×	交叉点	√	×	计算 Grid 中的交叉点	构建 Grid、泛洪查询	交叉点存储事件及信源
SAR	×	×	×	×	无需	泛洪路由请求及衡量 QoS 参数	存储扩展树上的父节点及 QoS 参数
Chang, et al.	最优	×	×	×	计算代价函数	衡量邻节点代价	存储邻节点代价
TinyOS Beaconing	×	×	×	×	无需	泛洪路由请求	存储扩展树上的父节点
Ye, et al.	最优	×	×	×	比较邻节点代价	广播代价	存储自身代价

9.3.3　路由协议的设计原则

路由协议主要设计目标是能源有效性路径的建立和可靠数据转发机制的形成。采用基于能耗的路由可以提高能量效率,加快网络冗余数据的收敛。无线传感器网络没有一个全局的标识,一般是基于属性的寻址方式,通常采用按需的被动式路由方式。由于传感器网络资源严重受限,目前提出的路由协议主要围绕着减少能量消耗延长网络生命周期而进行设计的。

因此,路由协议要遵循以下设计原则:

(1)无线传感器网络节点能量有限,所以路由协议设计必须将有效利用能源放在第一位,将服务质量 QoS 放在第二位考虑。

(2)不能执行复杂计算,要求路由协议的帧和算法简单有效,实现的程序代码短,路由表项尽可能少。

(3)不能在节点保存太多的状态信息,且节点间不能交换太多的路由信息。

(4)以多跳方式选择能量有效路由,转发数据帧。

(5)尽量避免发送冗余信息,减少能量的浪费。

为了避免单个节点的失效影响整个网络的效率,要求每个节点尽可能维护多条路由,维护多条路由是指每个节点同时维护至 Sink 节点的多条路由,只有当所有路径都失效时,才按需发起路由请求过程,从而降低了路由请求频率、分组等待延时和协议开销。

9.4　基于优先级的 PMRP 多径路由算法

最短路径或最小跳数路由可通过路径维护的方式提高网络寿命,但当在路径上未出

现死亡节点前,一直使用该路径进行路由。对于具有关节点①且关节点担任中继的连通网络而言,容易引起关节点早死,进而导致网络分割、不连通。

若在源节点和 Sink 之间建立多条候选路径,按照一定准则在多条路径上切换路由,让执行中继任务的能耗均衡到候选路径的节点上,则可在降低总能耗基础上,提高能耗均衡性,避免某个中继节点能耗过大而过早死亡。此外,当源节点感知数据流量较大时,通过在源节点和 Sink 节点之间的多径同时路由,能在一定程度上降低网络拥塞,提高带宽利用率。

9.4.1 PMRP 多径路由算法原理

本节从上述思想出发,提出一种基于优先级的 PMRP(Priority based Multi-path Routing Protocol)多径路由算法。其原理是在源节点和 Sink 节点间发现多个路径,并根据链路质量、剩余能量、跳数限制以及通信代价等参数对路径优先级排序,从中选择优先级最高的作为当前路径。

【定义 9.1】Sink 节点的邻节点。在 Sink 节点的通信范围内,能和 Sink 节点直接单跳通信的节点。

源节点要将感知数据上报给 Sink 节点,总要经过 Sink 节点的邻节点。对于某一网络拓扑结构,Sink 节点的邻节点可能有多个,这些节点和 Sink 节点之间通信代价各异。

【定义 9.2】链路质量。链路上成功传输的数据包与总发送数据包的比例,用 Link_reliability 表示。

链路质量是影响网络总能耗、能耗均衡性和传输可靠性的重要因素。在低质量链路上传输数据会增加重传能耗,低质量链路也会导致最短路径效率的降低。文献[13]对室内环境、野外环境及空旷区域的链路质量进行试验测试研究,结果表明:链路质量受电磁环境影响,有较强的时变性和不对称性。

对所有链路进行定时或实时估计的代价较大,只需对重要链路(如关节点、Sink 节点的相邻节点所在链路)进行实时估计,减少用于链路估计的控制报文开销。为了在链路质量的实时估计和定时估计之间折中,文献[14]提出利用窗口平均的指数加权滑动平均模型 WMEWMA(t,α),计算周期 t 内平均链路质量,并用 $\alpha \in [0,1]$ 平滑前一个时窗的链路质量。据此,链路质量估计为

$$\hat{Q}_{k+1} = \alpha \hat{Q}_k + (1-\alpha)\frac{\text{received}}{\text{received} + \text{failed}} \tag{9.2}$$

式中:$\hat{Q}_k$、$\hat{Q}_{k+1}$分别为 k 和 $k+1$ 时刻链路质量估计;received 为单位时间内接收节点收到来自发送节点的数据包数,failed 为丢失的数据包数。

调节 t 和 α 的值,可产生不同的估计效果:采用较大的 t 与 α,得到稳定估计;采用较小的 t 与 α,得到灵敏估计。

本算法链路质量估计方法:Sink 节点的邻节点在向 Sink 节点转发感知数据时,还发送用于链路质量估计的报文。Sink 节点根据式(9.2)估计与自己相邻节点的链路质量,

---

① 关节点又称瓶颈节点,当断开与关节点相连的所有通信链路时,网络分割为几个不连通的子网。

避免对每条路径上的所有链路质量估计，降低报文开销。

【定义 9.3】Sink 节点邻节点的剩余能量。Sink 节点的邻节点初始能量与已消耗能量之差，用 E_residual 表示。

在定义 9.1 ~ 9.3 的基础上，提出源节点和 Sink 节点之间能耗高效的 PMRP 多径路由算法。针对不同应用类型，路径发现和维护过程如下。

当 Sink 节点需要查询某个节点的感知信息时，路径发现过程为 Sink 节点先根据网络拓扑判断邻节点数及位置，再向其邻节点广播包含 Sink 节点位置的 Hello 消息，邻节点在收到该消息后，向 Sink 节点返回应答消息，据此 Sink 节点可判断邻节点剩余能量和链路质量。然后运用 Dijkstra 算法搜索出源节点至所有邻节点的代价最小路径，并根据邻节点剩余能量、链路质量和代价进行加权，对候选路径进行决策，从中选择优先级最高的作为当前路径，并将结果广播给区域内的节点。工作一段时间后，若某个路径上出现死亡节点，Sink 根据网络拓扑结构和代价重新选择路径。

当网络执行连续监测或事件驱动型监测任务时，源节点先通过逐级广播的方式，将含有源节点位置信息的数据包发送给 Sink 节点，这样 Sink 节点就可知道事件发生的区域，即知道了源节点位置，据此可执行与查询过程类似的路径发现与维护操作。

在路径发现过程中，Sink 节点先向邻节点广播 Hello 消息，并且邻节点需向 Sink 节点返回反映其剩余能量和链路质量的应答消息，这会产生一定的报文开销。PMRP 路由算法伪代码如表 9.4 所列。

表 9.4　PMRP 路由算法伪代码

```
<1> initialization of network: N、R、E、data_rate;
<2> //randomly deploy cluster head and Sink in the detection region
        CH_x = rand(N); CH_y = rand(N); S_x = rand(1); S_y = rand(1);
<3> //Judge the connectivity of backbone network
for(i = 1;i <= N;i++)
{
  Calculate distance between Cluster head and Sink CH_to_Sink(i);
    if(CH_to_Sink(i) <= R)
      CH i and Sink are neighbors;
  for (j = 1;j <= N;j++)
    {
      Calculate distance between Cluster head i and j CH_to_CH(i,j);
      if(CH_to_CH(i,j) <= R)
        CH i and j are neighbors;
    }
}
<4> //Find the optimal paths among Sink's neighbor cluster head and source cluster head;
        Dijkstra(Souce cluster head, Sink's neighbor cluster);
<5> //multi-path selection
      Path_Priority = a1 × E_residual + a2 × Link_reliability + a3/Path_Cost
    Select current routing path based on its priority;
    if(Path_Priorit(i) == Path_Priorit(j))
```

（续）

```
      Select min hop_count;  //对于优先级相等的两个路径,选择跳数少的
    Sink broadcast routing decision to cluster heads;
<6 > Perform packet routing and calculate residual energy;
<7 >//Judge the working status of relay nodes based on E_residual
    if(E_residual > = E_threshold)
      relay node is still alive;
      Return to step <5 >;
    else
      relay node is dead;
    //judge the number of dead nodes
      if((N-dead heads) > = min number of heads that maintain the connectivity of network)
      Return to step <3 >;
    else
      Network is useless, quit;
```

在计算候选路径优先级时，需对剩余能量、链路质量和以距离 4 次方和表示的路径代价进行归一化处理，过程为

$$
\begin{cases}
\text{Link_reliability} = \text{WMEWMA}(t,\alpha) \\
\text{E_residual} = \dfrac{\text{E} - \text{E_dissipation}}{\text{E}} \\
\text{Path_cost} = \dfrac{\sum \text{Hop_Distance}^4}{\max(\sum \text{Hop_Distance}^4)} \\
\text{Path_Priority} = a_1 \times \text{E_residual} + a_2 \times \text{Link_reliability} + a_3/\text{Path_Cost}
\end{cases}
\tag{9.3}
$$

式中：a_1、a_2 和 a_3 为权系数，为了均衡上述 3 个因素对选路的影响，通常取 $a_1 = a_2 = a_3$。当两个候选路径的优先级相等时，选择跳数少的路径进行路由。

9.4.2 PMRP 算法仿真

将 40 个节点随机均匀分布在 100m × 100m 的监测区域内，节点通信半径 R_c 为 20m，源节点和 Sink 节点的位置随机产生。每个节点初始能量为 0.05J，剩余能量根据收发数据包能耗模型计算。

链路质量估计采用区间[0, 1]内的随机数，权系数 $a_1 = a_2 = a_3 = 1/3$。根据表 9.4 中的伪代码，编写仿真程序，路径选择过程如图 9.12 所示。

从图 9.12(a)来看，Sink 节点有 3 个邻节点，在源节点和 Sink 间存在 3 条候选路径。图 9.12(b) ~ 图 9.12(d)分别为网络运行 1537、4739 和 7053 轮时，从 3 条候选路径中选择的优先级最高的路径作为当前路径。

采用相同的拓扑结构、能耗模型和流量模型，分别对最小跳数、最短路及 PMRP 多径路由算法第一个节点死亡轮数和网络失效轮数进行统计。其中，第一个节点死亡轮数反映了能耗均衡性；网络失效轮数反映了网络总能耗。网络参数及仿真结果如图 9.13 所示。从第一个节点死亡和网络失效轮数看，PMRP 优于其他两种单径路由。

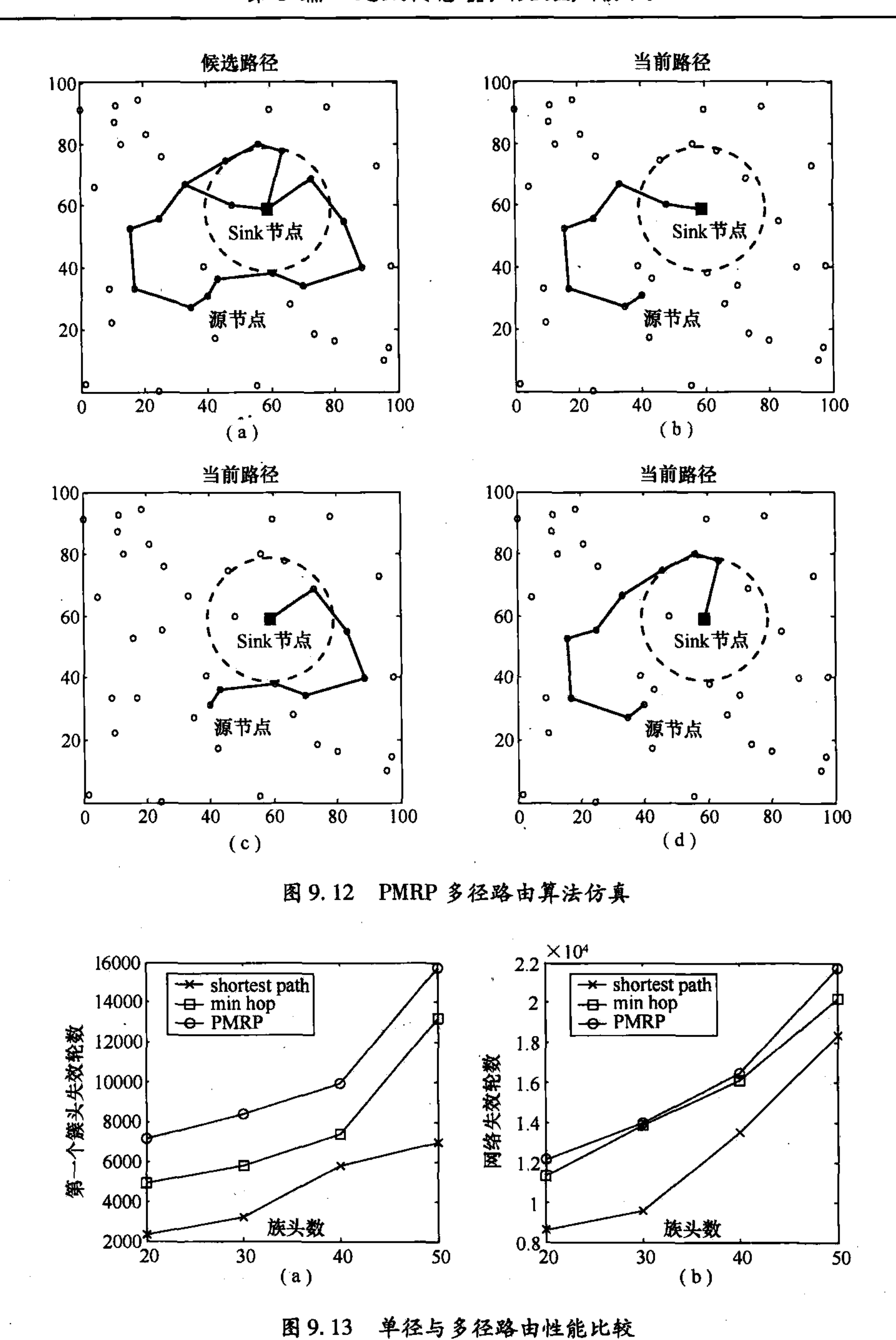


图 9.12　PMRP 多径路由算法仿真

图 9.13　单径与多径路由性能比较

9.5　基于动态负载均衡树的 DLBTP 路由算法

直观上看,多源单汇路由可看作多个单源单汇路由的合成,若能找出每个源节点和 Sink 节点之间的最短路,便找到了所有源节点到 Sink 节点的最短路。图 9.14 是一种简单的多源单汇路由,当各条路上的中继节点不产生流量且各路径不共享某个中继节点时,

这种方式是可行的。当部分节点作为源节点时,还可将这类多源单汇路由问题转为求解图的最小 Steiner 树。图的 Steiner 树是一棵连接所有给定节点子集的子树,最小 Steiner 树是指包含源节点和 Sink 节点的代价最小子树。求解最小 Steiner 树是 NP 完全问题,产生最小 Steiner 树需要指数复杂度的算法。

当中继节点也执行感知任务而产生流量时,特别是所有节点都作为源节点产生流量时,中继节点既要转发源节点的流量,也要发送自身的流量。在这种情况下,所有节点都并发的产生流量。对 Sink 节点而言,具有周期性数据收集、多对一的流量和多跳通信等特征,使得网络流量呈现出漏斗效应。即距离 Sink 节点远的节点流量小,距离 Sink 节点近的节点由于需要转发大量数据,流量较大、容易产生拥塞。图 9.15 是无线传感器网络流量具有漏斗效应的示意图。

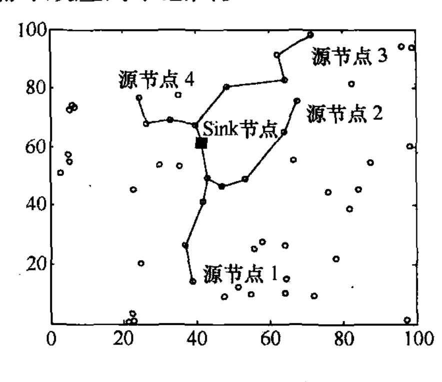


图 9.14　简单的多源单汇路由

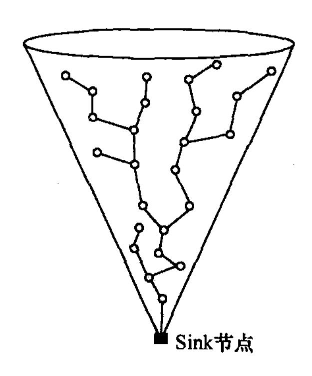


图 9.15　漏斗效应

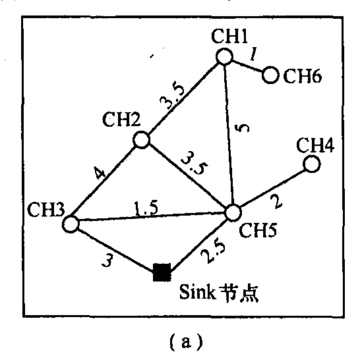
虽然在中继节点上采用数据聚集的方法,将多个单位流量聚集为一个单位流量,可减少总流量,并降低路由算法的复杂性。这一方法的缺点也很明显:每跳的延迟具有不确定性,难以设计对延时容忍的聚集算法[15];另外,网络在分簇过程中,每个簇有各自的监测区域,同一簇内的成员节点感知数据具有相似性,但簇间的感知数据则不然。许多应用都需要簇头将未和其他簇头聚集的原始感知数据上报到 Sink 节点,由 Sink 节点执行全网的融合。为此,如何设计能量高效的路由算法,使负载在全网范围内得到均衡,是多源单汇路由的关键问题。

针对所有节点都并发产生流量时的路由问题,许多协议或算法[16-20]都是构建以 Sink 节点为根的生成树,将代价最小的路径优化转化为求连通图的最小生成树。

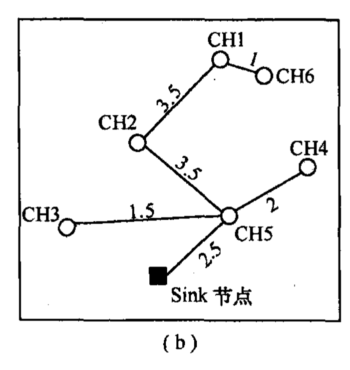
采用最小生成树形成路由路径时,虽能保证所有节点至 Sink 节点的总代价最小,但当 Sink 节点的通信范围内有多个节点时,最小生成树可能只经过其中一个节点。该节点由于长期执行中继任务,会快速消耗能量而死亡,导致网络分割或路径失效,需要重新建立路由路径。另外,最小生成树中每条树枝的长度可能有差异,当节点与 Sink 节点间的跳数差异较大时,各个树枝感知数据的传输延迟也就有差异,不利于数据聚集。

在图 9.16(a)所示的网络中,CH3 和 CH5 均在 Sink 节点的通信范围内。根据最小生成树规则建立路由路径时,CH5 被选作和 Sink 节点进行一跳通信,而 CH3 则需经过 CH5 和 Sink 节点进行两跳通信,所形成的最小生成树如图 9.16(b)所示。当 CH5 由于长期执行中继任务而死亡时,CH4 便成为孤立点。CH2 也会由于过多的承担转发任务而提早死亡,网络能耗均衡性和流量公平性不好。

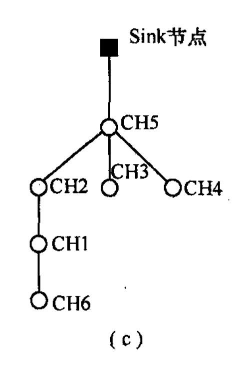
从图 9.16(c)来看,树枝 CH6→CH1→CH2→CH5→Sink 节点较长,共 4 跳;但树枝 CH3→CH5→Sink 节点和 CH4→CH5→Sink 节点只有 2 跳。这种结构虽然保证了经过所有顶点的路径代价最小,但各个树枝经过的顶点数有差异,引起节点的感知数据传输延迟的不确定性,不利于 Sink 节点进行全局融合。总之,纯粹的最小生成树虽可保证总代价最小,但能耗均衡性不好。



(a)



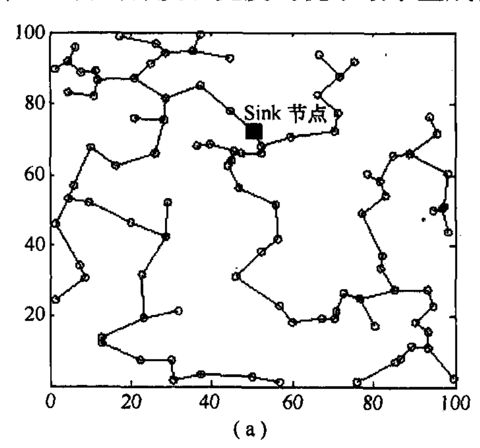
(b)



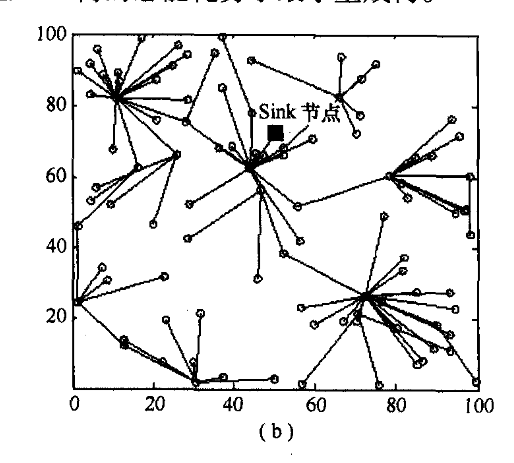
(c)

图 9.16　最小生成树示意图

在众多生成树中,宽度优先搜索树(Breadth First Search Tree, BFST)的深度最小、宽度最宽。图 9.17 是相同网络拓扑结构对应的最小生成树和 BFS 树,从负载均衡角度来看,BFS 树的深度和宽度均优于最小生成树,但 BFS 树的总能耗劣于最小生成树。



(a)



(b)

图 9.17　相同网络拓扑对应的最小生成树与 BFS 树

(a)最小生成树;(b)BFS 树。

为了解决负载均衡问题,Dai 在文献[17]提出一种以节点为中心的负载均衡树构造算法,但该方法仅适用于 Grid 布置的传感器网络,不具有通用性,且构造的是静态负载均衡树。Chen 等人[18]提出先用广度优先搜索算法在源节点和 Sink 节点之间建立广度优先树,在此基础上,动态调整子节点和父节点。

Yang 在文献[19]中提出 DQEB(Dynamic Query-tree Energy Balancing)协议,以节点剩余能量为权值,动态调整树的结构,将剩余能量较低的非叶节点转换成叶节点,实现负载均衡。DQEB 协议解决的是以 Sink 节点为根的广播树负载均衡问题,而非数据收集树的均衡。在 DQEB 协议中,Sink 节点向区域内的节点广播查询消息,非叶节点在转发查询消

息过程中，不产生新的感知数据。这种动态调整树结构的方法，不适用于所有节点都产生感知数据的多源单汇路由。

Zhang 等人[20]将传感器网络看成数据供需网络，Sink 节点是唯一的最终数据需求者，传感节点是数据生产者和运输者，数据需求者从生产者处购买数据。基于这一思想，在 Sink 节点与节点以及节点与节点之间建立起平衡的供需关系，将 Sink 节点和节点组织成负载平衡网络。可见，基于图论中树的概念，多源单汇路由的核心就是构建综合考虑负载均衡和总能耗的路由树。

9.5.1 DLBTP 路由算法原理

本节结合 BFS 树和最小生成树的特点，提出动态负载均衡树(Dynamic Load Balanced Tree Protocol, DLBTP)路由算法。DLBTP 路由算法在初始 BFS 树基础上，利用负载均衡度的概念，通过嫁接与局部调整树结构的方式构建负载均衡树。既可提高路由的负载均衡性，又兼顾路由过程中总能耗的最小性，且与 BFS 树及最小生成树相比，计算复杂度无明显增加。

基于负载均衡树的 DLBTP 路由算法以负载均衡树建立与维护为核心，分为初始化、负载均衡树建立、稳定传输和负载均衡树维护 4 个阶段。

初始化阶段：根据网络连通性，生成以 Sink 节点为根的初始 BFS 树。

负载均衡树建立阶段：先对初始 BFS 树进行嫁接，再根据负载均衡度，调整部分节点与其父节点或子节点的关系，对负载均衡树局部调整。

稳定传输阶段：节点通过负载均衡树向 Sink 节点发送感知数据，并估计各簇头剩余能量。

负载均衡树维护阶段：当有节点因能耗过大而死亡时，网络连通性发生变化。返回初始化阶段，根据某个节点死亡后的网络拓扑，重新产生初始 BFS 树。

【定义 9.6】叶节点：只发送自身感知数据，无后代的节点。

【定义 9.7】非节点：既发送自身感知数据，又需转发后代节点感知数据，有后代的节点。

根据多跳路由的流量特点，子节点多的非叶节点需转发的数据包多；反之越少，特别是叶节点，由于无子簇头，只需发送自身的感知数据。

【定义 9.8】子树路由代价(Sub Tree Cost, STC)：以 Sink 节点邻节点为根的第 i 棵子树中，每个节点完成一次向 Sink 节点发送长度为 l 感知数据的能耗，用 $\mathrm{STC}(i)$ 表示。

【定义 9.9】负载均衡度(Load Balance Degree, LBD)：每个子树路由代价和的平方与路由代价平方和的 k 倍(k 为子树数目或 Sink 节点邻节点数目)之比，用 LBD 表示，其表达式为

$$\mathrm{LBD} = \frac{\left[\sum_{i=1}^{k} \mathrm{STC}(i)\right]^2}{k\sum_{i=1}^{k} \mathrm{STC}(i)^2} \tag{9.4}$$

负载均衡度的定义来源于切比雪夫不等式，对于实数域上的序列 $a = \{a_1, a_2, \cdots,$

$a_k\}$，有 $k\sum_{i=1}^{k}a_i^2 \geqslant (\sum_{i=1}^{k}a_i)^2$，当且仅当 $a_1 = a_2 = \cdots = a_k$ 时，等式成立。对于式(9.4)，当且仅当 STC(1) = STC(2) = ⋯ = STC(k) 时，LBD = 1。即当每棵子树路由代价均相等时，负载均衡度为 1，否则小于 1。

负载均衡树的构建包括嫁接和局部调整两个过程。

1. 负载均衡树的嫁接

Sink 节点根据网络拓扑结构产生初始 BFS 树后，将网络拓扑和 BFS 树的结构广播给区域内的节点。各节点据此广播，可获得父节点编号 Parent_ID、邻节点列表 Neighbor_list、距离 Sink 节点的跳数 hop_count、子节点数目 Child_num 以及子簇头节点编号 Child_ID 等参数值，并将这些值保存在存储器中。

Sink 节点的每个邻节点根据 Parent_ID 判断自身是否已和 Sink 节点建立直接通信，若 Sink 节点的某个邻节点的父节点不是 Sink 节点，表明该节点寄生在其他簇头下，未和 Sink 节点建立直接通信，则需将以该节点为根的子树断开，嫁接到 Sink 节点上。

在嫁接过程中，邻节点先向其父节点发出退去请求消息 Quit_Message，格式为 <ID, Child_num>，其中：ID 为当前邻节点编号，对于父节点而言是它的一个 Child_ID；Child_num 为当前邻节点的子节点数目。父节点在收到该消息后，先根据 ID 判断发出退出请求消息的节点是否真是自己的子节点，若是子节点，则将该节点从 Child_ID 中删除，并将 Child_num 减少 1；否则不应答该消息。然后，给邻节点返回确认消息 ACK，表明父节点已同意其退出。

收到 ACK 消息后，当前邻节点由于在 Sink 节点的单跳通信范围内，可直接向 Sink 节点发送请求加入消息 Enroll_Message，格式为 <ID>。因为树的嫁接是以邻节点为根的整个子树枝的嫁接，Sink 节点只需知道 ID 就可根据初始 BFS 树判断请求加入的邻节点的子树结构。嫁接成功后，Sink 节点向该邻节点返回 ACK 消息。收到 ACK 后，以当前邻节点为根的子树中的节点重新在局部更新属性值。在各种属性中，只有 hop_count 发生变化，嫁接后的跳数为 hop_count = hop_count − 根节点的初始跳数 + 1。嫁接过程伪代码如表 9.5 所列。

表 9.5　负载均衡树嫁接过程伪代码

```
<1> initialization: Current ID←Parent_ID, Neighbor_list, hop_count, Child_num, Child_ID;
<2> for each neighbor of Sink
      {
        if(Parent_ID! =Sink)
        {
          Send Quit_Message to Parent;        //向父节点发送退出请求
      }
      ......
      //父节点的应答程序
<3>  if(ID is wrong)
        {
          Exit Program;                       //身份验证
        }
```

（续）

```
    else
      Reply ACK to Current ID;           //身份确认后返回 ACK 消息
      Delete Child_ID;                   //将当前节点从子节点中删除
      Child_num = Child_num - 1;         //修改相应参数值
  ……
    Send Enroll_Message to Sink;         //当前节点向 Sin 发送加入请求
<4> for each offspring of Sink's current neighbor
    {
        hop_count = hop_count - initial hop count of Current ID + 1;
      }                                  //成功加入后,修改 hop_count 值
    }
```

通过嫁接的方法，可形成与 Sink 节点的邻节点数目相等且以 Sink 节点的邻节点为根的子树。这种嫁接过程是在局部进行的，不影响其他邻节点的子树结构，因此无需 Sink 节点重新向区域内的簇头广播新的树结构。整个过程仅需收发 4 个控制报文，消息复杂度低。

在图 9.18 所示的初始 BFS 树中，共有 13 个簇头参与路由，其中，CH1、CH2、CH3 和 CH9 是 Sink 节点的邻簇头，能和 Sink 节点单跳通信。而以 CH9 为根的子树寄生在 CH1 的子树中，这样负载出现明显的不均衡性。通过嫁接过程，CH9 向其父簇头 CH7 发送 Quit_Message = <CH9, 2>，CH7 收到该消息后，断开 CH7 和 CH9 的通信链路。CH9 再向 Sink 节点发送 Enroll_Message = <CH9>，在 CH9 和 Sink 节点间建立通信，在一定程度上均衡负载。

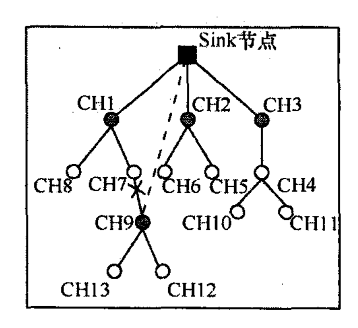


图 9.18　子树的嫁接

2. 负载均衡树的局部调整

初始 BFS 树经嫁接后，负载均衡性虽有所改善，但子树间的路由代价仍会有较大差异。树的局部调整过程就是通过调节子树间相邻节点的隶属情况，最大化 LBD 的过程。

Sink 先计算每棵子树的代价与 LBD 值，当 LBD 小于设定的阈值时，从叶节点数较多的子树中随机选择一个叶节点，根据 Neighbor_list，将其调整到其他子树中。重新计算子树的代价与 LBD 值：若 LBD 增加，则接收局部调整；否则，放弃该调整，从叶节点中选择其他节点。重复上述过程，直到 LBD 达到设定的阈值为止。局部调整算法伪代码如表 9.6 所列。

表 9.6　负载均衡树局部调整伪代码

```
<1> for (round; round <= set value; round ++)
    {
    for each sub_tree
      {
      calculate STC(i), LBD;        //计算每棵子树的代价
      }
<2> if(LBD >= threshold)
    {
    Exit;                           //LBD 满足要求时退出
```

（续）

```
    }
  else
    Randomly choose a non - leaf cluster head;
    Connect it with other sub_tree;    //局部调整树结构,重新计算 STC(i)
}
```

9.5.2 DLBTP 路由算法仿真

为便于直观看出仿真过程中树结构的变化，只将 20 个节点随机均匀布置在 100m × 100m 的正方形区域中，节点的通信半径 $R_c = 30$m。

分别对 Sink 节点位于正方形区域中心和区域边缘两种情形进行仿真，验证动态负载均衡树路由算法的性能。Sink 节点位于正方形区域中心时，网络负载均衡树的调整过程如图 9.19 所示，虚线圆内的节点是 Sink 节点的邻节点。

在图 9.19(a) 所示的初始 BFS 树中，Sink 节点有 4 个邻节点，但只有两个和 Sink 节点直接建立了通信，以另外两个邻节点为根的子树则寄生在其他节点下。

嫁接后的负载均衡树如图 9.19(b) 所示，其中，粗实线为新建立的通信链路。图 9.19(c) 为负载均衡度经迭代达到阈值时的负载均衡树，经过 749 轮稳定传输后，第一个节点死亡，网络仍连通。

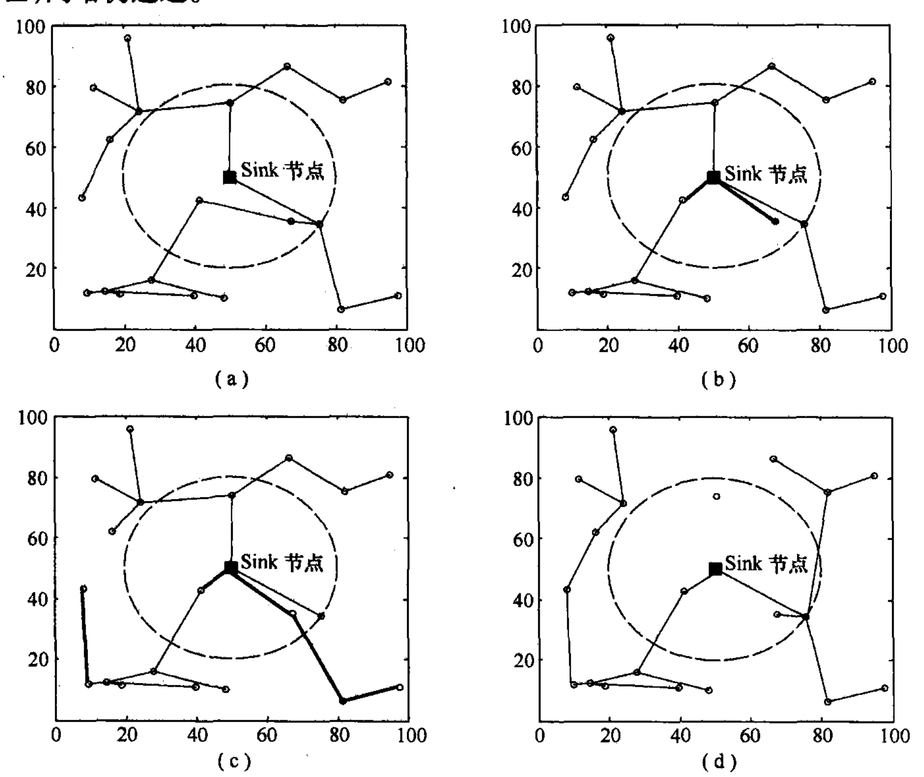


图 9.19　Sink 位于区域中心时负载均衡树的构建

(a) 初始 BFS 树；(b) 嫁接后的负载均衡树；

(c) 局部调整后的负载均衡树；(d) 第一个簇头死亡后的 BFS 树。

图 9.20 为 Sink 节点位于区域边缘,坐标为(100, 50)时,动态负载均衡树路由算法对 BFS 树的嫁接和调整过程。对于这种拓扑结构,Sink 节点的邻节点转发流量均衡性不如 Sink 节点位于区域中心时的均衡性好,当 Sink 节点的一个邻簇头死亡后,网络失效。

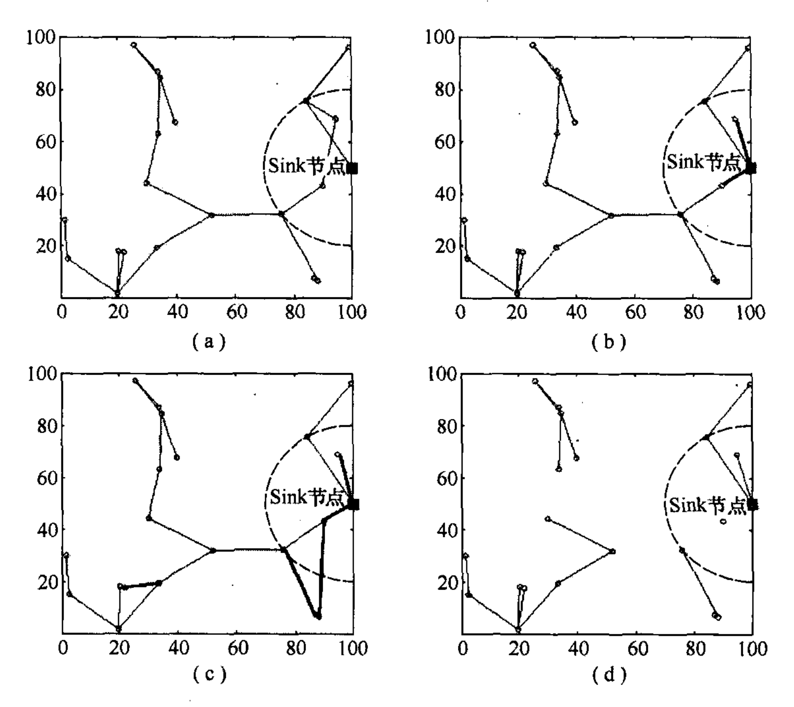


图 9.20　Sink 位于区域边缘时负载均衡树的构建

(a)初始 BFS 树;(b)嫁接后的负载均衡树;

(c)局部调整后的负载均衡树;(d)第一个簇头死亡后的 BFS 树。

对于相同的节点布置和能耗模型,分别比较 MST、BFS 树和 DLBTP 路由算法在 Sink 节点位置不同时的性能,结果如表 9.7 所列。

表 9.7　多源单汇路由算法性能对比

Sink 节点位置	负载均衡度			第一个簇头死亡轮数		
	MST	BFS 树	DLBTP	MST	BFS 树	DLBTP
(50, 50)	0.065283	0.16610	0.25571	463	612	749
(0, 50)	0.012855	0.13044	0.20685	317	439	573
(50, 0)	0.013969	0.16897	0.21836	195	362	607
(50, 100)	0.052475	0.13967	0.23182	301	410	612
(100, 50)	0.025639	0.12941	0.20667	135	233	451

在 Sink 节点位置相同时,从负载均衡度和第一个节点节点死亡轮数来看,均符合 DLBTP > BFS 树 > MST;另外,对于相同的节点布置,Sink 节点位于区域中心时,对于同一生成树算法,其性能优于 Sink 节点位于其他位置时的性能。

9.6 无尺度混合跳分层路由协议

为了解决如何高效利用有限网络资源和如何提高网络拓扑动态变化适应性的问题，考虑节点数量多和易失效的特点，以简单性、节能性、鲁棒性和可扩展性为原则，提出一种无尺度单跳—多跳层次型路由协议（Free Scale Ssingle-Multi Hop routing protocol, FSSMH），实现给定网络拓扑结构模型下的数据路由和网络连通。

9.6.1 网络分层路由的数学模型

无线传感器网络分层路由的数学模型可描述如下：网络可抽象为一个无向图 $G=(V,E)$，V 表示网络中节点集，E 表示两个节点间的双向通信链路集。节点数为 M，传感器节点和簇头节点集合有 B 个节点，Sink 节点有 1 个。对于无向图 $G=(V,E)'$，有正整数 g，满足 $1\leqslant |V| \leqslant g$。

【定义 9.10】一个层次深度为 $L(L\geqslant 1)$ 的网络结构模式是 V 的集合，它可以表示为 $V=\{P_1, P_2, \cdots, P_L\}$，$P_L$ 表示第 L 层节点的集合，显然有 $|V|=\sum_{i=1}^{L} P_i$。

【定义 9.11】$P_i=\{v_1, v_2, \cdots, v_x\}$ 表示为第 i 层中节点的集合，$C_i=\{v_{ij}\}$ 表示第 i 个簇中的节点集合，其中，v_{i0} 表示簇头节点，v_{ij} 表示传感器节点，显然有 $|P_i|=\sum_{i} |C_i|$。对于 P_i 层中的任意一个簇结构满足以下条件：

(1) $\cup_{i=1}^{n} C_i = P_i$，每一个节点分属不同的簇。

(2) $|C_i \cap C_j| = \phi$，任两个簇之间没有交集，即同一节点不能同属不同的簇。

(3) $|C_i| \geqslant 2$，任一个簇中的节点数目必须大于或等于 2，且有一个簇头节点。

【定义 9.12】E 中的代价函数为

$$C=f(N_n, V_p, T_p) \tag{9.5}$$

式中：N_n 为传输单位数据能量消耗代价；V_p 为路径剩余信道容量（带宽）；T_p 为路径平均延迟时间。

【定义 9.13】无线传感器网络路由实质上是在有限能源约束下寻找最小代价的传输路径问题，即

$$\min \sum_{j=1} C(h) + P(h) \quad (N_p \leqslant N_{\max}) \tag{9.6}$$

式中：h 为传输路径中的跳数；$N_{\max}$ 为节点的最大能量；$P(h)$ 为路由节点处理每条路径帧的代价，$P(h)=hy+\frac{h}{u}$；y 为转发单位帧的代价；u 为处理单位帧的代价。

【定义 9.14】按照 $L \sim \ln(M)$ 分布原则，网络层数为

$$L=\ln(M)+1 \tag{9.7}$$

本文结构设计、仿真及平台验证均采用 $L=2$ 的分层模式，所有传感器节点的集合为“第 1 层”、所有簇头节点的集合为“第 2 层”、Sink 节点为第 3 层。

9.6.2 FSSMH 路由协议相关阐述

1. 无线传感器路由协议相关定义

【定义 9.15】无尺度(Free Scale):网络 N 中的节点度服从幂律分布,某个特定度的节点数目与这个特定度之间的关系可用一个幂函数近似表示,则这种节点度的分布称为无尺度。实证研究发现,大量实际网络可以被认为是无尺度网络[23]。

【定义 9.16】同心环带(Concentric Zone):以簇头节点为圆心,在簇内作等间隔圆环,相邻圆环之间形成的环带为同心环带。

【定义 9.17】时间复杂度(Time Complexity):算法在选定参与转发数据帧的节点所消耗时间的量级。

【定义 9.18】消息复杂度(Message Complexity):算法在选定参与转发数据帧的节点所发送分组数的量级。

【定义 9.19】消息域(Message Field):算法在选定参与转发数据帧的节点时所必须知道的拓扑图信息范围。

其中,时间复杂度和消息复杂度是衡量无线传感器网络协议和算法的重要指标,也是无线传感器网络设计成败的门槛标准。

2. 被动路由与分层路由

被动路由也称按需路由。在动态变化的网络环境中,被动路由不事先生成路由,仅在传感器节点或簇头节点需要时才"按需"搜索到 Sink 节点的路由,其优点是不需要周期性的路由信息广播,节省了一定的网络资源,提高了网络生命周期;缺点是发送数据分组时,Sink 节点具有可达不确定性和路由发现引起延时的不确定性。典型协议有 AODV(Ad hoc On-Demand Vector Routing)、DSR(Dynamic Source Routing)、ABR(Associativity-Based Routing)等,而 AODV 是 DSR 和主动路由 DSDV(Destination Sequenced Distance Vector)的综合,具有内存和物理开销较低、主动路由的时延很小和扩展性较好的优点,且实现简单。被动路由协议主要由路由发现和路由维护两个过程组成。当传感器节点需要获得到 Sink 节点的路由,而该路由又没有在路由表中时,路由发现过程被激活,路由节点(传感器节点或簇头节点)采用"广播"方式,向整个网络广播路由请求分组,当有路由请求帧到达 Sink 节点时,Sink 节点将向传感器节点或簇头节点发出路由请求应答帧。这样,在传感器节点或簇头节点与 Sink 节点之间会建立起双向活动路径,随着拓扑结构的变化,当活动路径上的某段链路失效断开时,路由维护过程被启动。

分层路由基于簇进行层次划分,若干相邻传感器节点构成一级簇,每个簇有一个簇头,簇与簇之间通过簇头节点通信,所有簇头构成二级簇,并与 Sink 节点通信。层次路由协议混合了主动路由和被动路由协议的优点。典型协议有 CGSR(Clusterhead Gateway Switch Routing)、ZRP(Zone Routing Protocol)。分层路由协议比较适合于无线传感器网络,分层设计可以大大减少网络流量,达到节约能耗的目的。分层路由协议包括簇形成协议、簇维护协议、簇内路由协议和簇间路由协议 4 个部分。

在层次式路由协议中,网络拓扑结构的细节通过节点间的层层聚合被隐藏起来,降低了网络的存储要求和通信载荷,同时路由信息分层传播,也降低了全局广播次数。现有层次型主要路由协议:LEACH,它是一个典型聚类层次的单跳路由协议;TEEN,它是基于能

量效率的阈值敏感传感器网络协议，是改进的 LEACH 协议；PEGASIS[8]，它是在 LEACH 协议基础上采用无通信量的簇头选举机制建立的协议；TTDD 主要是解决网络中存在多 Sink 节点及其移动问题。

3. 路由协议设计目标的几点假设

(1)节点间不存在单向链路，节点间可双向通信，每个节点均采用全向天线。

(2)传感器节点与簇头节点数目已知，各环带邻居传感器节点之间可相互通信，传送包括采集数据、ID 号、剩余能量、故障询问与应答等信息，簇头节点均可与簇内的传感器节点通信，Sink 节点为单节点，可与通信半径内的簇头节点通信。

(3)每个同构传感器节点和簇头节点初始都具备相同的功能，且各节点的初始能量值相等，簇头节点的能源能够承担作为网络骨干节点的任务。

(4)传感器节点被随机均匀分布在一个规定的平面区域内，感知数据获取只与节点的通信半径和能量有关。

(5)只考虑数据通信、数据处理和路由建立开销，忽略传感器节点感知、状态变迁和路由维持开销，忽略这些能量开销的依据是网络中传感器节点和簇头节点各自是同构的。

4. FSSMH 路由协议的无尺度含义

从宏观上看，无线传感器网络的数据传输遵循多对一的模式，属于收敛播(Convergecast)。

从路由策略类型讲，无尺度路由是一种被动路由协议；从逻辑拓扑结构讲，是一种层次式路由协议，且具有多路径的特点。

出于固定目标的要求，除了原有节点失效和新节点加入外，拓扑结构基本不发生变化，因此没有必要花费很大的代价频繁地更新路由表信息。由于节点状态变迁而引起拓扑结构变化的过程中，也遵循无尺度的偏好依附原则，传感器节点优先连接节点度高的簇头节点。

网络邻近节点间采集的数据具有相似性，存在冗余数据，网络中簇头节点具有数据融合能力，冗余数据经数据融合处理后再进行路由，因此，网络中数据帧所含信息量无法用统一的尺度衡量，也是无尺度的。簇头节点发送数据帧所包含的信息量远远大于传感器节点的信息量。

网络无尺度路由用于解决节点易于失效，且节点的处理能力、存储能力和通信能力有限的路由问题。

由于幂函数曲线是一条下降相对缓慢的曲线，因此，网络中度小的节点是传感器节点，度大的节点是簇头节点和 Sink 节点。

9.6.3　FSSMH 路由协议设计

基于前述假设和被动路由协议 AODV 基础上，实现 FSSMH 路由协议。该协议将无线传感器网络构造成无尺度拓扑结构网络，并进行数据路由。

FSSMH 协议包括无尺度簇形成协议、多路由簇维护协议、簇内路由协议和簇间路由协议。无尺度簇形成协议是解决如何在分布式无线传感器网络环境下使传感器节点高效地聚集成簇，该部分协议是 FSSMH 路由协议的关键。多路由簇维护协议解决在节点状态变迁过程中所引起的拓扑结构变化，包括维护节点失效和新节点加入、新簇

产生和消亡等功能。簇内和簇间路由协议通过最优化路径完成数据从传感器节点到 Sink 节点的传输。

1. FSSMH 算法设计

FSSMH 协议是一种被动式的层次式路由协议，只有当需要传输数据时才会查找路由，大大减少了网络中的协议帧。FSSMH 协议使用一种类似于传统路由表的“路由入口表”来维护路由信息，每个目的地一个路由项，路由项用目的地址的逻辑地址代表，通过这种方式能有效避免环路，并确保保存的路由是最新的。路由入口表包含内容：目的节点逻辑地址；到达目的节点跳数；下一跳逻辑地址；路由过期时间。

FSSMH 路由算法包含 3 个方面的内容：路由发现、路由维护和路由失效。簇头节点是路由算法实现的核心节点，当它要向 Sink 节点发送数据帧而没有可用路由时，向所有邻居节点广播一个 RRF 帧进行路由发现，RRF 帧通过网络传播，所有转发 RRF 帧的簇头节点会建立一条逆向路由路径，收到 RRF 帧后的 Sink 节点应答 REF 帧，REF 到达路由请求节点后，则创建一条到 Sink 节点的路由表项。若一定时间内仍没有 REF 帧应答，则中止路由发现过程。当路由项建立成功后，节点周期性地向路由项中下一跳节点发送 HMF 消息以维护路由，一定时间内未收到应答，则认为下一跳链路失效，发送 REA 协议帧，启动路由维护，若其他邻居节点存在有效路径，则以该节点作为路由下一跳建立新连接，算法流程描述如图 9.21 所示。

FSSMH算法流程	
1	Sink节点通过广播对网络节点进行分层，并获得整个网络所有节点能量状况
2	第二层中的簇头节点运行广播算法，获得通信半径内的传感节点和邻居簇头节点信息
3	第一层中的传感节点按照无尺度偏好依附原则，同通信半径的簇头节点形成多个紧密连接的簇，并将感知信息发给簇头节点
4	簇头节点对数据进行融合后，直接或通过邻居簇头间接发给 Sink节点
5	簇头如果通过邻居簇头节点转发信息，则重复该步骤，直到数据到达Sink节点
6	故障节点诊断及上报
7	网络绝大多数节点能源耗尽，等待重新构建

```
if 网络节点失效
  if 簇头失效 then
    上传故障报警信息，等待簇头更换
      if 所有簇功能失效 then
        跳转 (7)
    else if 传感节点失效
  邻居节点感知，簇头节点实时报告给Sink节点
  end if
end if
```

图 9.21　FSSMH 算法流程

路由协议中帧类型可分为网络帧、层内帧、簇内帧和层间帧。网络帧的作用域为整个无线传感器网络，层内帧的作用域为层内所有节点，簇内帧的作用域为簇内所有节点，层间帧的作用域为网络中不同层间通信，层间帧包括路由创建、路由维护、路由失效和层间数据传输等协议。

2. 无尺度簇形成协议

由于 Sink 节点能源不受限制，运算和存储能力都很强，可运行复杂算法，而且对全网状况有着更全面的了解，可生成最优的簇类。合理的利用 Sink 节点，将会有效的提高网

络的吞吐量。

在时间域内,把网络整个数据处理过程按时间维度细分成不同的回合,每个回合由簇形成阶段和数据传输阶段组成。网络生命初期,节点能源较为充裕,为了获得较好的吞吐量,采用集中式簇类形成过程,利用 Sink 节点的优势,由 Sink 节点按照当前网络拓扑和不同节点的能源分布情况,将整个网络划分成不同的簇,每个簇类由一个簇头节点和若干传感器节点组成。簇内传感器节点采用广播的形式发送自身信息和采集的数据,内环邻居节点和簇头节点接收“控制与状态信息”和“采集数据”,而同环内邻居节点仅接收除采集信息之外的其他信息,簇头节点进行数据融合后再向 Sink 节点传输数据。最优簇生成完毕,Sink 节点便知道网络中每个节点的当前状态,如节点的 ID 号、位置、可用能源等信息。

无尺度簇形成协议利用 Sink 节点把原本地位平等的传感器节点和簇头节点按照平面位置、能源情况和任务属性,划分为不同的层次,依据定义(9.15)和定义(9.16)快速构建无尺度拓扑结构,创建过程示意图如图 9.22 所示。

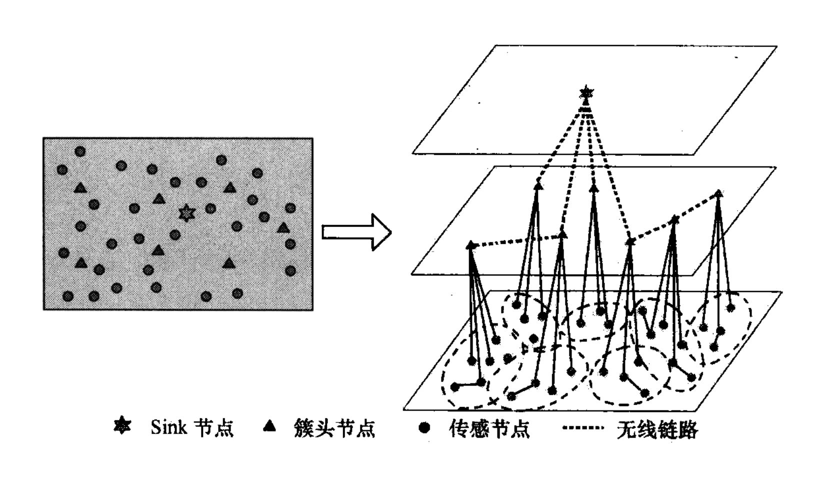


图 9.22　层次式拓扑结构创建过程

在网络生命周期的后期,节点能源较为贫乏,为了得到更长的网络生命周期,转而采用分布式自协商簇类形成过程,即 Sink 节点不再参与簇的形成,而由传感器节点通过广播,加入新的簇,再进行数据传输。

3. 多路由簇维护协议

多路由簇维护协议要解决在节点状态变迁过程中的簇结构维护,其中包括节点退出和加入簇,簇产生和消亡等。

(1)传感器节点能量即将耗尽时(低于一定阈值),传感器节点发送告警信息给簇头,簇头及时上传给 Sink 节点,等待修复。

(2)若传感器节点出现硬故障或软故障,簇头节点无法根据故障诊断协议判断节点状况时,则等待指定时间后认为节点失效,上传 Sink 节点等待修复。

(3)为保证路由的可靠性,每个簇类的传感器节点都在成簇阶段维护一个邻居簇头节点的信息,一旦本簇的簇头节点由于异常原因失效,传感器节点立即加入邻居簇头节点的簇,通过多跳路由保证了路由的健壮性。

在簇头节点发生硬故障和软故障而失效后，邻居簇头可通过诊断算法及时发现节点故障，并上报 Sink 节点，等待技术人员的修复和更换。

9.6.4　FSSMH 路由协议仿真试验与性能评价

为验证本文提出的 FSSMH 路由协议的算法有效性，采用仿真进行测试。仿真使用本课题开发的无线传感器网络模拟器所建立的路由算法仿真模型，对其进行评估验证协议的可行性。无线传感器网络模拟器的仿真环境如图 9.23 所示，仿真场景布置与输出结果如图 9.24 所示。

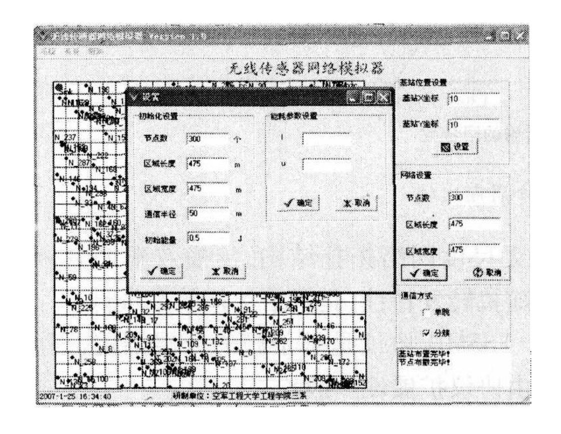


图 9.23　模拟器的仿真环境

图 9.24　场景布置与输出结果

(1)仿真模型。本节的仿真场景为 475m×475m 的一个区域，区域内均匀分布 300 个节点，每个节点具有 0.5J 的初始化能量，节点的通信半径为 50m，节点的通信速率为 100Kb/s，帧固定长度为 128bit。按照 FSSMH 路由协议的设计原则和 LEACH 路由协议不能少于 5 个簇的规定，仿真试验将网络化分为 12 个簇，每个簇内有一个簇头节点和 24 个传感器节点，各节点均有收发功能。场景中同时仅设一个 Sink 节点用来接收簇头节点发来的感知数据。

(2)仿真功能。根据网络体系结构的层次，基础层逻辑物理发送和接收接口采用 GFSK 调制方式和曼彻斯特编码，传感器节点数据帧大小和产生时间周期由预先编写的程序实现，用以模拟周期性的感知数据；无线标准采用 TDMA 通信方式；数据融合单独设置一个模块用以嵌入融合算法，所有嵌入的模块均采用 C++代码。

(3)仿真模型验证。在对路由算法仿真试验之前，首先进行模型的有效性验证。在设置好相关参数和模块后，启动仿真过程，仿真过程由事先设置的传感器节点周期性帧驱动，并按照嵌入模拟器的 FSSMH 路由算法触发路由发现、路由应答过程，生成网络拓扑结构，并完成路由选择、帧转发。传感器节点模块和簇头节点模块能将产生的模拟数据有效的传输到 Sink 节点，并将 Sink 节点统计的数据流量实现后台保存，数据流量包括数据帧量、网络节点数量、节点能耗、时间延迟等信息。经过测试，仿真模型可以完成 FSSMH 路由协议的性能评估。

测试和评价主要是在 FSSMH 路由协议和典型的路由协议之间进行，对比的路由协议为最为经典和简单的传统网络路由协议 Flooding 和 Gossip，第一个提出数据聚合的层次

路由协议 LEACH。测试和评价的尺度为定义(9.17)~定义(9.19)。

1. 网络整体性能综合评价

网络生命周期:从图 9.25 看出,由于 FSSMH 协议采用了无尺度拓扑结构和簇内数据融合技术,平均能耗较低,网络生存时间最长,而 Flooding 和 Gossip 协议盲目利用资源的特性,大量消耗了节点能量,网络生存时间最短。

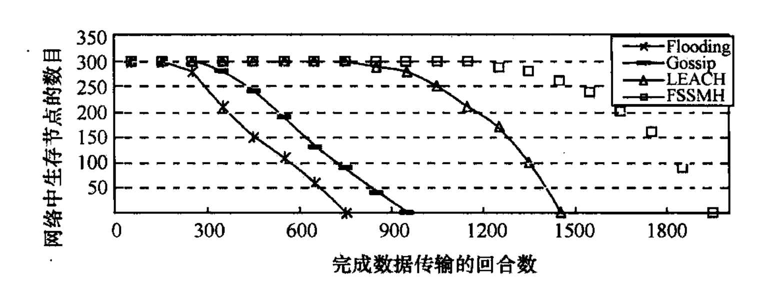


图 9.25　网络生命周期比较

网络传播效率:由于 FSSMH 协议形成的是无尺度网络拓扑结构,传播效率最高,而 Flooding 和 Gossip 协议"内爆"与"交叠"广播和随机转发特性,是网络传播效率最低。

网络扩展性:从图 9.26 仿真结果看出,由于 FSSMH 协议是基于簇的分层结构,因此扩展性好,而 Flooding、Gossip 和 LEACH 三种路由协议扩展性一般。

网络延迟性:从图 9.27 看出,随着网络节点规模的增大,各种协议平均时延均有所增大,由于 Flooding 和 Gossip 算法泛洪传播冗余信息,因此平均时延增加显著,而层次型协议普遍时延较小,FSSMH 略好于 LEACH。

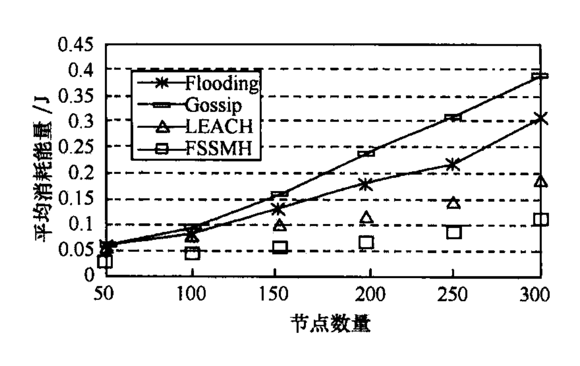


图 9.26　网络扩展性比较

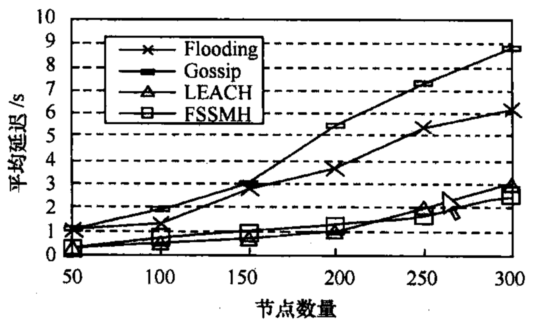


图 9.27　网络延迟性比较

算法实现复杂度:由于 Flooding 为广播算法,Gossip 为随机发送算法,因此都容易实现,而层次式协议 FSSMH 和 LEACH 的实现相对复杂。

2. 感知数据有效性与可靠性评价

在模拟器中设定模型的仿真时间为 1000 × 120ms,即在产生数据周期的 120ms 内,可产生 1000 个模拟数据帧,总计产生 1000 × 300 个数据帧。以 Sink 节点收到帧后的某一时刻开始计时,Sink 节点收到的有效数据帧统计结果如表 9.8 所列,帧数对比如图 9.28 所示。由表 9.8 得到表 9.9 和图 9.29 不同协议的可靠性分析。

表 9.8 不同算法下 Sink 节点收到的有效帧数

仿真时间/ms	数据帧数			
	Flooding	Gossip	LEACH	FSSMH
20	40163	33288	39616	16331
40	84166	58675	80171	31335
60	103265	77136	115299	50238
80	116442	105168	138852	58336
100	121633	110871	153563	62887
120	125566	116112	160112	71702

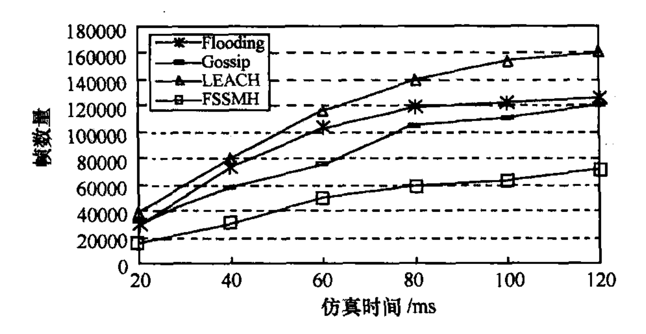


图 9.28 Sink 节点收到帧数对比图

表 9.9 不同协议可靠性

仿真时间/ms	可靠性/%			
	Flooding	Gossip	LEACH	FSSMH
20	80.37	66.58	79.24	89.52
40	84.22	58.68	80.17	92.33
60	68.84	51.42	76.87	91.84
80	59.22	52.61	76.78	91.16
100	48.85	44.34	64.04	90.38
120	41.85	40.37	53.37	89.19
平均可靠性/%	63.89	52.33	71.74	90.75

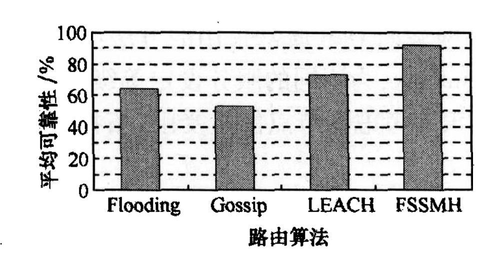


图 9.29 不同算法可靠性对比图

由表9.10和图9.29可知：

(1)由于FSSMH协议中建立了无尺度的拓扑结构，并采用了簇内数据融合，网络中数据帧流量及到达Sink节点的数据帧数比其他3种协议都降低了很多，且可靠性达到了90.75%。

(2)Flooding协议具有冗余度功能，所以在仿真周期前一阶段Sink节点收到帧数量最多，可靠性也最高，但在仿真周期的后一阶段由于节点能量耗费太大，大部分节点功能失效，所以Sink节点帧数量趋势下降，即可靠性明显下降。

(3)Gossip协议中邻居节点的随机选取造成数据帧一定程度上的丢失，并且由于帧发送代价较高，仿真时间末期有一部分节点失效，因此算法可靠性最低。

(4)LEACH算法中采用数据聚合的分层方法创建网络拓扑结构，因此数据帧可靠性较高，但由于采用一跳通信，所以在生命周期后期节点能量下降很多，可靠性呈下降趋势。

9.7　路由协议面临的挑战与有待解决的问题

9.7.1　路由协议面临的挑战

目前，对路由算法的研究都是在节省能源的基础上多方位、多角度开展的。路由机制不仅考虑到转发数据需要的总能量，更能从整个网络系统的角度，考虑网络系统能量的均衡使用，延长整个网络的生存时间。

尽管在路由算法的研究方面取得了很多进展，但还有一些根本性的问题有待进一步研究。

(1)在不维护全局信息的前提下，构建能量有效的全局最优路由策略。由于无线传感器网络受能量约束、处理能力有限和无线通信带宽窄等限制，传感节点难以获得整个网络的拓扑信息，无法采用传统的全局中心控制式路由算法精确计算优化路径以达到全局最优。针对此问题，Estrin提出一类特殊的分布式算法，要求网络中的每个节点只与一跳范围内的邻节点交互，即本地化算法。本地化算法具有简单、鲁棒和可扩展等优点，但由于只能获得局部信息，因此大部分路由只能达到局部优化，难以实现全局最优的目标。

(2)路由算法的QoS支持。无线传感器网络中的QoS支持问题是如何动态地配置网络资源使数据传输效率更高。与无线自组织网络不同的是，无线传感器网络不仅要考虑在拓扑结构和信道状态频繁变化的环境中实现QoS，还要考虑在降低能耗和QoS间达到平衡的问题。目前，为保障网络的QoS通常采用的方法：沿着特点应用数据流经过的路径，预留端到端的资源，如IntServ；为不同的服务设定等级，对等级高的服务做特殊处理，如DiffServ。这两种方法均没有考虑到节点能量受限、拓扑结构动态变化、无线多跳通信的特点，因此需要予以改进。

(3)路由算法的安全与认证机制。路由协议通过广播多跳的方式实现数据交换。没有受到保护的路由信息容易遭受多种形式的攻击。目前，很少有路由协议考虑安全问题。虽然人们对结构与无线传感器网络相似的无线自组织网络安全问题进行了深入的研究，并设计了多种加密与认证机制，但这些机制大都基于公钥密码。由于公钥

密码的通信开销较大，因此不适合在资源受限的无线传感器网络中使用。此外，由于无线传感器网络本身在安全方面的弱点和应用环境的多样性，使得在设计它的安全机制时，面临很多困难。

(4)在节点能量分布不均衡的前提下，构造能源有效的路由策略。无线传感器网络作为一个数据采集网络，绝大部分信息是由各个节点流向汇聚点的。因此，流量分布不均匀，具体表现在源节点和目的节点的数量不对称，源节点多而目的节点单一；传输方向不对称，以汇聚点为目的的数据流远远超过以它为源的控制流。这种流量分布特点造成的结果是节点功耗分布极不均匀，越接近汇聚点，链路的流量越高，相应节点的负载越重，寿命就越短。因此，针对网络流量分布不均衡现象，构建节能的路由协议，以延长网络的生存时间仍需进一步研究。

9.7.2　路由协议有待解决的问题

在无线传感器网络中，由于网络内节点资源有限，数据包的传送需要通过多跳方式到达目的端，因此路由算法的选择是网络层设计的一个重要任务。

传统无线网络的路由协议设计以避免网络拥塞、保持网络的连通性和提高质量网络服务为主要目标。在路由实现过程中，首先利用网络层定义的逻辑上的网络地址来区别不同节点以便实现数据交换，然后通过路由选择算法决定到达目的地的最佳路径。与传统无线网络相比，虽然无线传感器网络具有与无线自组织网络极为相似的特征，但在网络特点、通信模式和数据传输需求方面却与传统无线网络有着很大的不同，具体体现在以下几个方面：

(1)能量受限的无线移动终端。无线传感器网络的一个重要特征就是能量受限。网络内每个传感节点通常使用容量有限、不可更换的电源，节点计算、通信和存储能力有限。

(2)以数据为中心的通信方式。与以地址为中心的网络相比，由于网内节点数量大、节点随机布置等特点，每个传感节点不需要使用全局唯一的标识或地址。

(3)邻节点数据的相似性。无线传感器网络邻节点监测的可能是同一个事件，如火灾，从不同监测点得到的数据具有较高的相似性。因此，邻节点的感知数据存在冗余性，采用一定的网内数据聚集技术可有效节省网络资源。

(4)应用相关性。传统网络发展的趋势是电信网、计算机网以及电视网的逐步融合，形成通用信息平台以满足各种应用需求。而在无线传感器网络中，传感节点和物理环境交互密切，无线传感器网络的通信构架及其所提供的服务都是针对每个特定应用而设计的。

(5)拓扑结构动态变化。在无线传感器网络中，由于能量限制、环境干扰和人为破坏等因素的影响，传感节点会经常破坏。由于节点的移动或损坏，加上无线发射装置发送功率的变化和信号之间的干扰，网络拓扑结构会频繁动态变化。

无线传感器网络的特点和通信需求要求路由协议在设计过程中必须以节约能量为首要目标，并采用折中机制，使用户可以在延长网络存活时间和提高网络吞吐量、降低通信延迟间做出选择。而传统网络路由协议设计的首要目标是提供高服务质量和高效利用网络带宽，其次才考虑能量的节约。

因此，传统路由协议不适合在无线传感器网络环境中运行，需要对其进行改进，提出

适合于无线传感器网络的路由协议。

参考文献

[1] 张劼，张宗麟，景博等．分布式无线传感器网络及其应用支撑技术研究[J]．装备指挥技术学院学报，2006. 6:79 – 83.

[2] Hedetniemi S, Liestman A. A survey of gossiping and broadcasting in communication networks. Networks, Vol. 18, No. 4, pp. 319 – 349. 1988.

[3] Kulik J, Heinzelman W R, Balakrishnan H. Negotiation-based protocols for disseminating information in wireless sensor networks. Wireless Networks, Volume: 8, pp. 169 – 185, 2002.

[4] Intanagonwiwat C, Govindan R, Estrin D. Directed diffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of ACM MobiCom'00, Boston, MA, 2000, pp. 56 – 67.

[5] Rodoplu V, Meng T H. Minimum Energy Mobile Wireless Networks, IEEE Journal Selected Areas in Communi-cations, vol. 17, no. 8, Aug. 1999, pp. 133 – 344.

[6] Xu Y, Heidemann J, Estrin D. Geography-informed Energy Conservation for Ad-hoc Routing, In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking 2001, pp. 70 – 84.

[7] Yu Y, Estrin D, Govindan R. Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks, UCLA Computer Science Department Technical Report, UCLA-CSD TR-01 – 0023, May 2001.

[8] Lindsey S, Raghavendra CS. PEGASIS: Power-efficient Gathering in Sensor Information Systems [J]. In: Proc. of the IEEE Aerospace Conf. Montana: IEEE Aerospace and Electronic Systems Society, 2002:1125 – 1130.

[9] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Mi-crosensor Networks, Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00), January 2000.

[10] Lindsev S, Raghavendra C S. Sivalingam K. Data gathering in sensor networks using the energy * delay metric[C], in: Proceedings of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[11] Manjeshwar A, Agrawal D P. TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks[C]. in: Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, 2001:2009 – 2015.

[12] 陈华容，张崇富．Bellman-Ford 算法的改进研究[J]．电子科技大学学报，2006,35(2): 29 – 213.

[13] Jerry Zhao, Ramesh Govindan. Understanding Packet Delivery Performance In Dense Wireless Sensor Networks[A]. SenSys'03[C], Los Angeles, California, USA, November 5 – 7, 2003.

[14] WOO A, TONG T, CULLER D. Taming the underlying challenges of reliable multi-hop routing in sensor networks [A]. Proceedings of the 3 rd ACM Conference on Embedded Networked Sensor Systems [C]. 2003:14 – 27.

[15] Shrivastava N, Buragohain C, Agrawat D. Medians and beyond: New aggregation techniques for sensor networks[A]. Proceedings of the 2nd ACM Conference on Embedded Networked Sensor System(SenSys)[C]. Baltimore: ACM Press, 2004:239 – 249.

[16] 杨挺，孙雨耕，田飞，等．基于最小生成超树的无线传感器网络路由算法研究[J]．传感技术学报，2007,20(4): 903 – 907.

[17] Dai H, Han R. A node-centric load balancing algorithm for wireless sensor networks[A]. Proceedings of the Global Telecommunications Conference (GLOBECOM)[C]. San Francisco: IEEE Press, 2003: 548 – 552.

[18] Tzung-Shi Chen, Hua-Wen Tsai, Chih-Ping Chu. Gathering-Load-Balanced Tree Protocol for Wireless Sensor Networks [A]. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing [C], 2006, 2: 8 – 13.

[19] Yang H, Ye F, Sikdar B. A dynamic query-tree energy balancing protocol for sensor networks[A]. Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)[C]. Atlanta:IEEE Press, 2004:1715 - 1720.

[20] Zhang CQ, Li ML, Wu MY. An approach for constructing load-balancing networks for data gathering wireless sensor networks[J]. Journal of Software, 2007,18(5):910 - 921.

[21] 张劼. 无线传感器网络体系结构及关键技术研究[D]. 西安:空军工程大学, 2007.

[22] Zhang Jie, Jing Bo, He Liming, etc. Mixed-Hop Hierarchical Routing Protocol Based on Scale-Free Network Topology, IEEE 2009 9th international conference on electronic measurement & instruments(ICEMI2009), 2009,8.

[23] Doherty L. Algorithms for Position and Data Recovery in Wireless Sensor Networks[D]. Department of Electronic Engineering and Computer Science, University of California, Berkeley, 2000.

第4篇

无线传感器应用支撑与关键技术

第 10 章　无线传感器网络时钟同步

时钟同步对任何分布式系统而言都是很重要的，无线传感器网络中许多算法或协议也需要节点间的时钟同步作为支撑[1]。在无线传感器网络的应用中，传感节点采集的数据如果没有空间和时间信息是无任何意义的。

准确的时间同步是实现传感器网络自身协议的运行、数据聚集、TDMA 调度、协同休眠、定位等的基础。例如，多个传感器联合来探测一个运动目标，如车辆或者坦克的轨迹，每个传感器将它观测到的位置和时间返回到处理中心，如果这些时钟不事先同步，那么无法判断观测到的位置的时序，从而无法计算出轨迹。在链路层采用时隙分配的 MAC 协议时，节点间如果不能保持时钟同步，会造成时隙混乱无法有效利用带宽资源。

10.1　时钟同步概述

对于无线传感器网络而言，节点的本地时钟 $H(t)$ 由特定频率的晶振和计数寄存器构成，每出现一定数量的振荡脉冲，寄存器值就增加 1，访问该寄存器便可知当前时间。在本地时钟基础上，可构造不同类型的软件时钟 $C(t)$，如 $C(t)=C(t_0)+f(H(t))$。由于低成本、低功耗和微型化的要求，节点采用的晶振性能差异较大，且晶振频率受电压、温度及使用时间等多种因素的影响，使晶振的实际工作频率与出厂标定值有差异，导致节点之间时钟不同步。

10.1.1　时钟模型

1. 速率恒定模型[2]

对于速率恒定模型，$r(t)=\frac{\mathrm{d}C(t)}{\mathrm{d}t}=$常数，即晶振频率为常值。当要求的时钟同步精度远低于频率变化引起的偏差时，该模型的假设是合理的。

2. 漂移有界模型

通常情况下，时钟速率 $r(t)$ 在一定范围内波动，即 $1-\rho\leqslant r(t)\leqslant 1+\rho$，其中，$\rho$ 为时钟漂移。对于低成本的网络节点而言，一般有 $\rho\in[1,100]$ ppm①。

3. 漂移变化有界模型

时钟漂移的变化 $\xi(t)=\frac{\mathrm{d}\rho(t)}{\mathrm{d}t}$是有界的，即 $-\xi_{\max}\leqslant\xi(t)\leqslant\xi_{\max}$。

对于节点 i 和 j，用 $C_i(t)$、$C_j(t)$ 表示它们在 t 时刻的时间值。若采用速率恒定模型，

---

① 当时钟漂移率为 1ppm 时，每 11 天会产生 1s 偏差；当漂移率为 100ppm 时，每 2.8h 就会产生 1s 偏差，Crossbow 的 Mote 节点平均漂移约为 40ppm。

$C_i(t)$可表示为 $C_i(t)=a_it+b_i$。由此可知，任意两个节点 i 和 j 的时钟满足如下线性关系：

$$C_i(t)=a_{ij}C_j(t)+b_{ij} \tag{10.1}$$

式中：a_{ij}、b_{ij}分别为相对漂移与相对偏移。

当两个节点的时钟保持同步，即 $C_i(t)=C_j(t)$时，$a_{ij}=1$、$b_{ij}=0$。因此，对于采用速率恒定时钟模型的场合，时钟同步就是对(a_{ij},b_{ij})进行估计，这样，两个节点在新的时刻便保持时钟同步。

10.1.2　时钟同步算法执行周期

选择合适的时钟同步算法执行周期很重要：过于频繁地执行时钟同步算法会占用一定的时间和带宽资源，特别是控制报文开销；但时钟同步算法执行的时间间隔过长时，时钟偏差不能满足相关应用对时钟同步的精度要求，进而影响相关协议和应用的性能。重要的是当节点间时钟偏差不满足协议和应用要求时，才执行时钟同步算法。下面推导时钟同步间隔与同步误差、时钟漂移率的关系。

若f为晶振工作频率（单位：MHz），ρ 为时钟漂移率，f_+、f_-分别为晶振的最大和最小工作频率，则

$$f_+=(1+\rho)f \tag{10.2}$$

$$f_-=(1-\rho)f \tag{10.3}$$

则节点间时钟周期偏差最大值为

$$T_\Delta=T_--T_+=\frac{1}{f_-}-\frac{1}{f_+}=\left(\frac{1}{1-\rho}-\frac{1}{1+\rho}\right)\frac{1}{f}=\frac{2\rho}{(1-\rho^2)f}\approx\frac{2\rho}{f} \tag{10.4}$$

累计同步误差为

$$t_\Delta=t_{\mathrm{sync}}T_\Delta f \tag{10.5}$$

式中：t_{sync}为两次时钟同步的时间间隔。

因此

$$t_{\mathrm{sync}}=\frac{t_\Delta}{T_\Delta f}\approx\frac{t_\Delta}{2\rho} \tag{10.6}$$

【例 10.1】若晶振时钟漂移率 $\rho=10\mathrm{ppm}$，时钟同步误差不大于 100μs，根据式(10.6)可得，时钟同步算法执行的时间间隔 $t_{\mathrm{sync}}=5\mathrm{s}$。

10.1.3　时钟同步评价指标

无线传感器网络中的时钟同步算法评价指标包括定量和定性两个方面。其中，定量指标包括同步精度、计算复杂度、收敛时间等；定性指标包括可扩展性、能量有效性、容错性和同步范围等。

同步精度：节点间以某一基准进行时间同步的偏差。

计算复杂度：算法在选定参与转发数据帧的节点所发送的分组数的量级。

协议收敛时间：时间同步算法在全网内完成一个轮回所用时间，即从网络时间发生变

化到网络上所有的相关节点都得知这一变化，并且相应地完成同步算法所需要的时间。

可扩展性：在传感器网络应用中，节点随机分布，因此分布密度通常不均匀，时钟同步机制必须能够适应这种网络范围和节点分布密度的变化。

能量有效性：由于电池能量的限制，对于无线传感器网络而言，要延长系统的生命周期，必须最小限度地且均匀地使用节点能量。为了减少能量消耗，应使网络时钟同步的交换信息尽可能得少，网络通信和计算处理的能耗应可预知，时钟同步机制应该根据网络节点的能量分布，均匀地使用网络节点的能量来达到能量的高效使用。

容错性：网络系统不顾某些节点所发生的时钟同步故障而继续运行的能力。

同步范围：局部同步或全局同步。

10.2　传统网络时钟同步算法

在传统网络中，已经提出了多种网络同步机制，C/S 模式是主要的时钟同步模式。客户端产生时钟同步请求消息，服务器回应时钟同步应答消息，通过测试这两个消息的发送和接收时间来估计两者的时间偏差，获得相对较精确的时钟同步。采用上述思想的典型例子就是网络时间协议 NTP[3]，被因特网用作网络时钟同步协议，NTPv4 精确度已达到毫秒级。实现方案是在网络上指定若干时钟源服务器，为用户提供授时服务，并且这些服务器之间能够相互比较校正，以提高准确度。

NTP 协议采用层次型树型结构，整个体系结构中有多棵树，每棵树的父节点都是一级时间基准服务器。NTP 协议要将时间信息从这些一级时间服务器传输到分布式系统的二级时间服务器成员和客户端，第三级时间服务器从第二级服务器获得时间信息，以此类推，服务器级数越小，越接近一级服务器，时间就越准确。由于 NTP 协议设计对象为因特网和计算机，设计重点为协议的可靠性和同步精度。该协议要求能够始终占用 CPU 资源，以便它可以执行连续的操作，使时钟一直保持同步，没有考虑能耗和计算能力问题，无法直接应用于无线传感器网络中。

在无线传感器网络应用中，节点对功耗有严格的要求，并且要求尽可能保持较小的外形尺寸和低廉的成本使其能够被大量部署，其部署环境经常是常人难以接近的恶劣环境，这使得部署后的维护通常是不可能的；显然将 GPS 和 NTP 用于无线传感器网络的时间同步是不可取的。分布式系统中对时间同步也有大量研究，但这些方法都没有考虑传感器网络的特点，需要较大的资源开销，所以不适合传感器网络的时间同步。鉴于时间同步在无线传感器网络应用中的基础性作用，必须研究适用于无线传感器网络的时间同步算法。

10.3　典型时钟同步算法

传统无线传感器网络时间同步协议可分为发送者—接收者同步和接收者—接收者同步两类。图 10.1(a)为发送者—接收者同步协议。发送者在报文中嵌入发送时刻而接收者记录下报文接收到的时刻，利用这些时刻信息可估算出收发双方的时间偏移，通过对时间偏移的补偿，达到收发双方的时间同步。可以看出，发送者—接收者同步协议的关键路径为从发送者应用程序层到接收者应用程序层。TPSN(Time Protocol for Sensor Networks)

协议[11]是典型的发送者—接收者同步协议，它通过 MAC 层时间戳技术及双向报文交换方法来抑制和减小传输延迟及延迟不确定性的影响。图 10.1(b)描述了接收者—接收者同步协议，与发送者—接收者同步协议不同，接收者—接收者同步协议的目的不是为了同步收发双方，而是去同步多个接收者。可以看出，相对于发送者—接收者同步协议，其关键路径缩短为从发送方物理层到接收方应用程序层。通过对同一个报文接收时刻的比较，接收者可以估算出它们之间的时间偏移。

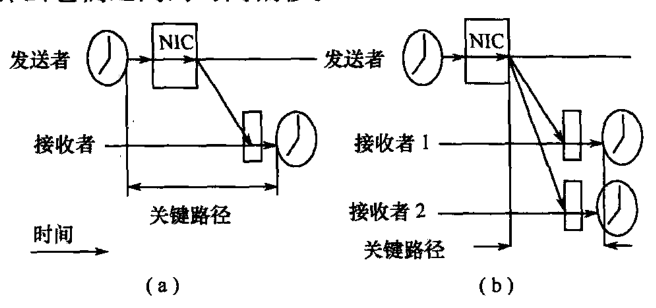


图 10.1　发送者—接收者同步协议与接收者—接收者同步协议

(a)发送者—接收者同步协议；(b)接收者—接收者同步协议。

节点之间为了达到同步需要交换各种各样的消息，受信道质量、节点工作环境和节点配置等因素的影响，同步消息在传输过程中的延迟具有不确定性，这是无线传感器网络时间同步的主要挑战之一。

同步消息从发送方要依次经过发送时间(Send Time)延迟、发送方 MAC 访问时间(Access Time)延迟、物理层传播(Propagation Time)延迟、接收方 MAC 层接收(Reception Time)延迟、接收方应用程序层(Receive Time)延迟，最终才能到达接收方的应用程序层。图 10.2 为同步消息传输延迟分解图，尽可能减小同步消息传输延迟的不确定性是提高同步精度的重要途径。

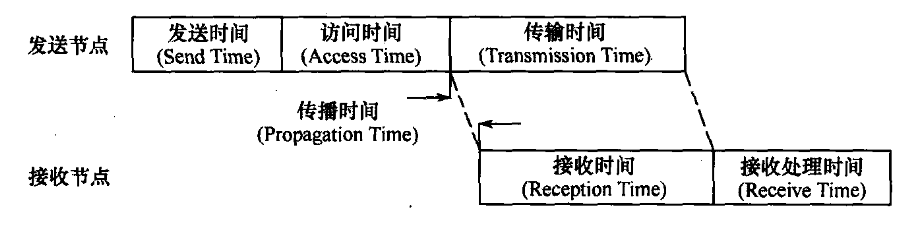


图 10.2　同步消息传输延迟分解

发送时间：用来产生同步消息并向 MAC 层提交发送请求，该过程的持续时间取决于当前处理器的载荷和操作系统的负担，因而具有不确定性；典型值为 0ms ~ 100ms。

访问时间：用来等待信道空闲的时间，依赖于网络的流量，也具有不确定性；典型值为 10ms ~ 500ms。

传输时间：用来传输同步消息的时间，取决于消息的长度和无线电波的传输速度，具有确定性；典型值为 10ms ~ 20ms。

传播时间：同步消息离开发送方至接收方的时间，取决于两者的距离，具有确定性，但该时间通常可忽略；典型值为 $<1\mu s$(距离 $<300m$)。

接收时间：与发送方的传输时间特性相同，且在同步消息传输过程中两者重叠；典型

值为 10ms ~ 20ms。

接收处理时间:接收方用来处理同步消息的时间,与发送时间的特性相同;典型值为 0ms ~ 100ms。

通过上述对传输延迟的分析,一般在发送方 MAC 层后对同步消息添加时间戳,接收方在接收时间后添加时间戳,以减少发送时间、访问时间和接收处理时间延迟的不确定性给同步精度带来的影响。

近年来,针对无线传感器网络的时钟同步问题,研究人员提出了近 10 种代表性的同步算法[4-9]。参考文献[10]从时钟同步的意义、无线传感器网络与无线网络、Ad hoc 网络和有线网络的区别出发,列举了多种同步算法的原理、应用场景及优缺点等。本节将这些同步机制和算法分为额外硬件支持、单向广播和双向成对同步 3 类。

10.3.1　额外硬件支持的时钟同步

在节点上安装 GPS 接收机,实现节点时钟与 UTC 同步是典型的额外硬件支持的同步方法。虽然 GPS 的时钟同步精度可达纳秒级,但 GPS 能耗大且某些情形下无法接收 GPS 信号,不适合大规模的无线传感器网络应用。

压控晶体振荡器(Voltage Control Oscillator ,VCO)时钟同步机制[4]利用参考时钟与节点本地时钟的偏差作为 PI 控制器的输入,控制器的输出为控制电压,用来控制 VCO 的输出频率。当本地时钟与参考时钟一致时,PI 控制器的输出为常值,VCO 的振荡频率亦为常值。

10.3.2　单向广播式时钟同步算法

单向广播式时钟同步典型算法有 RBS(Reference Broadcast Synchronization)[5]、DMTS (Delay Measurement Time Synchronization)[6]和 FTSP(Flooding Time Synchronization Protocol)[7]等。

RBS 算法是以“第三方广播”的思想让参照节点利用物理层广播周期性地向网络中其他节点发送参照广播(Reference Broadcast),广播域中的节点用自己的本地时钟记录各自的包接收时间,然后相互交换记录的时间信息,其过程如图 10.3 所示。

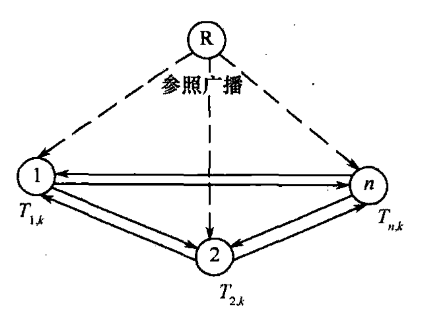


图 10.3　RBS 算法消息交换过程

这样,接收节点能够知道彼此之间的时钟偏移量,然后利用式(10.7)计算相对其他各个节点时钟偏移的平均值,并用它对本地时钟进行相应调整。当每个节点都获得相对其他节点时钟偏移量的平均值时,所有接收到同一参照广播消息的接收节点便获得了一个相对网络时间,即

$$\forall i \in n, j \in n, \text{offset}(i,j) = \frac{1}{m}\sum_{k=1}^{m}(T_{j,k} - T_{i,k}) \tag{10.7}$$

式中:n 为待同步节点数;m 为参考广播的次数;$T_{i,k}$为第 i 个节点接收第 k 个参考广播的本地时刻。

显然，由 offset(i,j)形成的矩阵为对称阵，且对角线元素为 0。

由于 RBS 采用接收者之间进行同步的方法，在关键路径中排除了发送方的发送时间和访问时间对同步精度造成的影响，使得广播同步机制得到比双向成对同步好得多的同步精度。

RBS 的缺点是对网络有一定的要求，不适合点对点通信的网络。节点间交换本地时间也需要额外的消息开销，对于由 n 个节点构成的单跳网络，需要 $O(n^2)$ 的消息交换。当 n 很大时，消息交换开销和节点的计算开销也非常大，扩展性差。另外，RBS 实现的是接收节点之间的时钟同步，未实现与参考节点的同步。

DMTS 算法引入时间戳(标记参考节点发送同步消息时刻)的概念，参考节点向区域内的节点广播带有时间戳的同步消息，接收节点通过精确地测量从发送节点到接收节点的单向时间延迟，结合发送节点中的时间戳计算时间调整值。这就避免了 RBS 算法中需要节点之间交换时钟信息且无法与参考节点的时钟保持同步的缺点，但 DMTS 是以牺牲时间同步精度换取较低的计算复杂度和消息复杂度。

DMTS 算法没有估计时钟的频率漂移，时钟保持同步的时间较短；也没有消除时钟计时对同步精度的影响，因而其精度不高，不适用于定位等要求高精度同步的应用。

FTSP 算法也是使用单向广播消息实现发送节点与接收节点之间的时间同步，但是算法的具体实现与 DMTS 有所不同。FTSP 采用参考节点多次广播带有发送时间戳的同步消息的方法，使每个节点获得多个(Global Time, Local Time)属性对，通过集中式线性回归法对时钟的相对漂移和相对偏移进行估计。FTSP 算法的消息交换过程如图 10.4 所示。

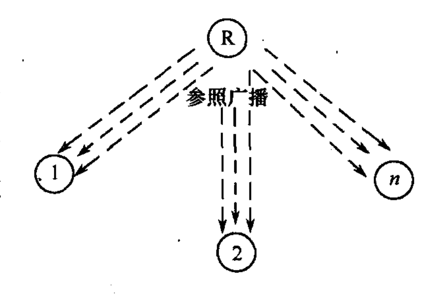


图 10.4　FTSP 算法消息交换过程

为了提高时间戳标记的精度，FTSP 算法通过对收发过程时延的分析，进一步降低了时延的不确定性。参考文献[12]认为，由于 FTSP 采用多个样本进行线性回归法来分析相对漂移和相对偏移，为了达到一定的估计精度，需要在节点上消耗大量的存储资源。

1. 相对漂移与相对偏移的回归分析

当同步消息在两个节点之间传输的时间可忽略时，由于 $C_i(t)$ 与 $C_j(t)$ 线性相关，若已知点集 $\{(C_i(t_k), C_j(t_k)) | 1 < k \leq n\}$，则可用线性回归法估计 a_{ij} 和 b_{ij}。

采用单向广播方式进行同步时，假设簇头的编号为 j，它在 $C_j(t_k)$ 时刻向簇内节点广播含有 $C_j(t_k)$ 时间戳的同步消息。成员节点 i 在 $C_i(t_k)$ 时刻收到该同步消息，这样，节点 i 就获得了参考时钟和自身时钟属性对 $(C_i(t_k), C_j(t_k))$。

利用线性回归法估计 a_{ij} 和 b_{ij} 时，满足方差最小原则，即式(10.8)取得最小值。

$$R = \sum_{k=1}^{n} [a_{ij} C_j(t_k) + b_{ij} - C_i(t_k)]^2 \tag{10.8}$$

为此，R 关于 a_{ij} 和 b_{ij} 的偏导数应为 0，即

$$\frac{\partial R}{\partial a_{ij}} = 2[a \sum_{k=1}^{n} C_j^2(t_k) + b \sum_{k=1}^{n} C_j(t_k) - \sum_{k=1}^{n} C_j(t_k) C_i(t_k)] = 0 \tag{10.9}$$

$$\frac{\partial R}{\partial b_{ij}} = 2\left[a\sum_{k=1}^{n} C_j(t_k) + nb - \sum_{k=1}^{n} C_i(t_k)\right] = 0 \tag{10.10}$$

将式(10.9)与式(10.10)改写成矩阵形式,有

$$\begin{bmatrix} \sum_{k=1}^{n} C_j^2(t_k) & \sum_{k=1}^{n} C_j(t_k) \\ \sum_{k=1}^{n} C_j(t_k) & n \end{bmatrix}\begin{bmatrix} a_{ij} \\ b_{ij} \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^{n} C_j(t_k)C_i(t_k) \\ \sum_{k=1}^{n} C_i(t_k) \end{bmatrix} \tag{10.11}$$

据此,可得

$$a_{ij} = \frac{n\sum_{k=1}^{n} C_j(t_k)C_i(t_k) - \sum_{k=1}^{n} C_j(t_k)\sum_{k=1}^{n} C_i(t_k)}{n\sum_{k=1}^{n} C_j^2(t_k) - \left[\sum_{k=1}^{n} C_j(t_k)\right]^2} \tag{10.12}$$

$$b_{ij} = \frac{\sum_{k=1}^{n} C_j^2(t_k)\sum_{k=1}^{n} C_i(t_k) - \sum_{k=1}^{n} C_j(t_k)\sum_{k=1}^{n} C_j(t_k)C_i(t_k)}{n\sum_{k=1}^{n} C_j^2(t_k) - \left[\sum_{k=1}^{n} C_j(t_k)\right]^2} \tag{10.13}$$

参考文献[12]认为,采用线性回归法估计相对漂移和相对偏移时,需以数组的形式在节点上保存一定数量的属性对$(C_i(t_k), C_j(t_k))$,以提高线性回归的精度,导致对存储器资源的开销较大。得出这一结论,主要是考虑进行求和运算时,属性对$(C_i(t_k), C_j(t_k))$必须静态地保存在存储器中,并通过循环的方式对数组中的元素进行求和运算。

在实际的单向广播同步过程中,可通过收发中断而非循环的方式进行求和运算。节点每接收一次同步消息,产生一次接收中断,读取无线芯片接收缓存中的同步消息,便可提取时间戳$C_j(t_k)$。从a_{ij}和b_{ij}的形式来看,包含4种类型的求和运算,分别为$\sum_{k=1}^{n} C_i(t_k)$、$\sum_{k=1}^{n} C_j(t_k)$、$\sum_{k=1}^{n} C_j(t_k)C_i(t_k)$和$\sum_{k=1}^{n} C_j^2(t_k)$。因此,用线性回归法估计相对漂移和相对偏移时,只需占用5个存储单元,其中4个用来保存求和运算的中间结果,一个用来保存无线芯片接收缓存中的时间戳。

利用回归法进行时钟同步可在线估计相对漂移和相对偏移,增加参考节点时钟同步消息的广播次数,可在一定程度上提高线性回归的精度。此外,由于节点间无需交换时间信息,也无需向参考节点返回消息,具有消息复杂度低、存储资源消耗少等优点。

2. 相对漂移与相对偏移的递推最小二乘估计

当同步消息在两个节点之间传输的时间不可忽略时,$C_i(t)$与$C_j(t)$满足如下关系:

$$C_i(t) = a_{ij}C_j(t) + b_{ij} + \varepsilon(t) \tag{10.14}$$

式中:$\varepsilon(t)$为同步消息的传输时间。

根据中心极限定理,当测量次数足够多时,$\varepsilon(t)$服从正态分布$\varepsilon(t) \sim N(0,\sigma^2)$。式(10.14)对应的矩阵形式为

$$
\begin{bmatrix} C_i(t_1) \\ C_i(t_2) \\ \vdots \\ C_i(t_k) \end{bmatrix} = \begin{bmatrix} 1 & C_j(t_1) \\ 1 & C_j(t_2) \\ & \vdots \\ 1 & C_j(t_k) \end{bmatrix} \begin{bmatrix} b_{ij} \\ a_{ij} \end{bmatrix} + \begin{bmatrix} \varepsilon(t_1) \\ \varepsilon(t_2) \\ \vdots \\ \varepsilon(t_k) \end{bmatrix} \tag{10.15}
$$

将式(10.15)改写为

$$
\begin{bmatrix} Z_1 \\ Z_2 \\ \vdots \\ Z_k \end{bmatrix} = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{bmatrix} X + \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_k \end{bmatrix} \tag{10.16}
$$

式(10.16)中,$Z_k = C_i(t_k)$;$H_k = [1, C_j(t_k)]$;$\boldsymbol{X} = [b_{ij}, a_{ij}]^{\mathrm{T}}$;$V_k = \varepsilon(t_k)$,且 $E[V_k] = 0$,$D(V_k) = \sigma^2$。这样,就将 b_{ij}与 a_{ij}的估计问题转化为最小二乘估计问题。最小二乘有集中式和递推式两种形式,考虑到无线传感器网络存储资源有限的特点,采用递推形式估计相对偏移和相对漂移。

式(10.16)对应的递推最小二乘估计为

$$
\begin{cases} \hat{\boldsymbol{X}}_{k+1} = \hat{\boldsymbol{X}}_k + \boldsymbol{P}_{k+1}\boldsymbol{H}_{k+1}^{\mathrm{T}}(\boldsymbol{Z}_{k+1} - \boldsymbol{H}_{k+1}\hat{\boldsymbol{X}}_k) \\ \boldsymbol{P}_{k+1} = \boldsymbol{P}_k - \boldsymbol{P}_k\boldsymbol{H}_{k+1}^{\mathrm{T}}(\boldsymbol{I} + \boldsymbol{H}_{k+1}\boldsymbol{P}_k\boldsymbol{H}_{k+1}^{\mathrm{T}})^{-1}\boldsymbol{H}_{k+1}\boldsymbol{P}_k \end{cases} \tag{10.17}
$$

在式(10.17)中,$\boldsymbol{P}_k$ 为 t_k 时刻的估计均方误差阵;虽然在 $\boldsymbol{P}_{k+1}$ 的递推过程中,存在 $(\boldsymbol{I} + \boldsymbol{H}_{k+1}\boldsymbol{P}_k\boldsymbol{H}_{k+1}^{\mathrm{T}})^{-1}$项,即矩阵求逆运算,由于 $\boldsymbol{H}_{k+1}\boldsymbol{P}_k\boldsymbol{H}_{k+1}^{\mathrm{T}}$为标量,因此求逆运算实为倒数运算,不会产生较大的计算复杂度。

10.3.3 双向成对时钟同步

双向成对同步典型代表有 TPSN[8]、Tiny-Sync/Mini-Sync[9]等,其基本原理如图 10.5 所示。

节点 i 在 T_1 时刻向节点 j 发送同步消息 SYNC_MSG,节点 j 用自身的时钟记录同步消息到达的时刻 T_2,则 $T_2 = T_1 + D + d$,其中,D 是消息传输时间;d 是节点之间的时钟偏移。然后,在 T_3 时刻节点 j 向节点 i 返回一个包含 T_2 与 T_3 的应答消息 ACK_MSG,节点 i 在 T_4 时刻收到该应答消息,则 $T_4 = T_3 + D - d$。若在发送同步消息和应答消息过程中的传输时间相同,通过式(10.8)可计算时钟偏移和传输时间。

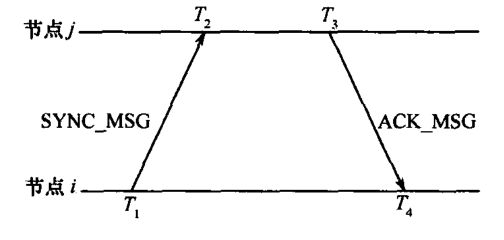


图 10.5　双向成对同步基本原理

$$
\begin{cases} d = \dfrac{(T_2 - T_1) - (T_4 - T_3)}{2} \\ D = \dfrac{(T_2 - T_1) + (T_4 - T_3)}{2} \end{cases} \tag{10.18}
$$

TPSN(Time Synchronization for Sensor Networks)算法是双向成对同步方法,分为层次发现阶段(Level Discovery Phase)和同步阶段(Synchronization Phase)两个阶段。

层次发现阶段的目的是在网络中产生一个分层的拓扑结构，并使每个节点都赋予一个层次号。

同步阶段的核心就是节点间成对的消息交换。该阶段由根节点的 time_sync 包发起，当接收到这个包，第一层的节点发起与根节点的双向消息交换。在发起消息交换之前，为最小化无线信道冲突，每个节点都要等待一个随机时间。一旦接收到根节点的应答消息，用式(10.18)计算它们之间的偏移和传播延迟，并调整自身时钟到根节点的时钟。第二层节点监听到第一层的一些节点与根节点的通信后，发起与第一层节点的双向消息交换，再一次需要等待一个随机时间以确保上层节点完成同步。这个过程最终使所有节点都与根节点同步。该过程中，下层节点不可避免地会与多个上层节点同步。

TPSN 算法的缺点是一旦根节点失效，就要重新选择根节点并重新进行上述两个过程，增加了计算和能量开销。同步阶段所用时间随节点数目的增加而线性增加。协议要求网络构造层次结构，使得它不适合于高度移动的节点。用泛洪广播方式构造层次树通信开销较大。

Tiny-Sync/Mini-Sync 是由北卡罗来纳州州立大学 Sichitiu 和 Veerarittiphan 于 2003 年提出的，该算法采用经典的双向成对同步机制，但数据处理方法不同，即固定值估计法。它假设节点的时间是真实时间的线性变化，时钟偏差和偏移在一段时间内是不变的。算法未采用式(10.18)计算时钟偏移，而是在节点 j 收到同步消息后立即返回应答消息，即 $T_3=T_2$。基于两个节点的时钟线性相关的假设，利用三元组(T_1,T_2,T_4)寻找线性关系中参数的上下界，从而确定相对漂移和偏移。

该方法的缺点是要多次交换 SYNC_MSG 和 ACK_MSG 才能获得多个三元组，这导致消息代价和存储代价都很高。

TSS(Time-Stamp Synchronization)同步协议是由 Frankfurt 大学 Kay Romer 于 2001 年提出的，在双向成对同步的基础上通过时间戳的转换来实现同步的典型算法。该算法提供按需的网内同步，步骤如下：首先确定时间戳在源节点处产生消息到达目的节点所经过的真实时间的上下界，然后把这个上下界区间转换为目的节点的时间，最后在目的节点处从消息到达时间中减去这个结果值。结果的时间区间指定了时间戳在源节点处产生到消息到达目的节点所经过的真实时间的上下界。时间戳的转换如下：

由式 $1-\rho\leqslant\frac{\Delta C}{\Delta t}\leqslant 1+\rho$（其中，$\Delta C$ 是节点本地时钟在真实时间 Δt 内的变化量，ρ 是节点时钟与理想时钟的频率差，即时钟偏差），可得

$$(1-\rho)\Delta t\leqslant\Delta C\leqslant(1+\rho)\Delta t \tag{10.19}$$

$$\frac{\Delta C}{1+\rho}\leqslant\Delta t\leqslant\frac{\Delta C}{1-\rho} \tag{10.20}$$

据式(10.19)和式(10.20)可以推出，Δt 时间内节点本地时钟差在$[(1-\rho)\Delta t,(1+\rho)\Delta t]$之间。

为使节点 i 的本地时间转换为节点在 j 的本地时间，首先通过真实时间区间 $\left[\frac{\Delta C}{1+\rho_i},\frac{\Delta C}{1-\rho_i}\right]$估计 Δt，然后通过$\left[\frac{\Delta C(1-\rho_j)}{1+\rho_i},\frac{\Delta C(1+\rho_j)}{1-\rho_i}\right]$来估计节点 j 相对真实时间的区间。

由于 TSS 算法还要确定时间戳寿命的范围，也包括每对节点间的消息延迟的估计。相邻节点间的消息延迟估计在区间[0,rtt]内，rtt 是消息在两节点间往返的时间。

根据图 10.6，消息 M2 相对发送者的延迟 d 可以通过下面的等式估计：

$$0 \leqslant d \leqslant (t_3 - t_2) - (t_6 - t_5)\frac{1-\rho_s}{1+\rho_r} \tag{10.21}$$

式中：$t_3 - t_2$ 是消息往返时间；$t_6 - t_5$ 是消息在接收方的存储时间。

随着消息在节点间的依次传输，每对节点间的往返时间 rtt 和消息在每个节点处的存储时间都累加起来估计时间戳的值。

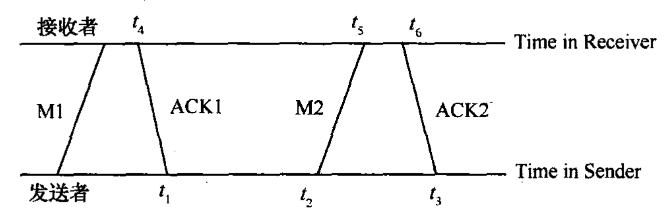


图 10.6　TSS 算法同步原理

该算法只在感兴趣时间发生时才同步节点的本地时钟，资源和消息开销比较低，适合于资源有限的无线传感器网络。最后的时间戳被限制在一定范围内。但同步误差随着包含时间戳的消息路径的跳数的增加而增加，在稀疏网络中跳数一般较多，这明显影响了同步精度。

萤火虫同步技术[13]对耦合延迟、耦合强度、耦合性质、初始相位、网络拓扑等隐私很敏感。虽然在两个振荡器的同步收敛性研究上取得一定进展，但无论是理论研究或模拟研究，研究者在某些结论上还不能达成一致。但有一点可以认同：在实际系统中，基于萤火虫同步策略的同步技术会取得一定误差范围内的同步。

上述算法都可以扩展到多跳情形，但同步精度与单跳情形相比略有降低，且随着跳数的增加，误差也增加。值得注意的是，双向成对时钟同步需要两个节点间分别交换消息，这就意味着在共享信道时由于 MAC 协议的不合理会导致信道冲突。

10.3.4　基于锁相环的时间同步机制与算法

考虑到无线传感器网络中由于节点和链路失效等因素导致拓扑结构动态变化的特点，以及为均衡能量损耗、延长网络生命周期而采用拓扑控制等系统性优化能耗的方案对网络带来的影响，文献[2]沿用 FTSP 中根节点的选取和维护方案[7]，着重讨论广播域内单跳同步机制与原理，在此基础上扩展到整个网络的多跳机制是较为直接和方便的。在一个广播域内，时钟参考节点（时标）周期性广播同步分组，分组中携带了时标节点的本地时钟，为避免广播分组在发送、访问信道和接收过程中由于系统和信道状态的不确定性因素可能引入的误差，采用在 MAC 层加盖时戳的方案[7,14]。收到同步分组的节点容易得到两个时钟间的差，FTSP 和 DMTS 直接用差值进行了偏移补偿。如果能通过分析这个差值时间序列，得到两个时钟相对漂移的信息，一次完成偏移和漂移补偿，则这样的时间同步算法会更有效率。因为它不会再像 FTSP 那样，为了进行线性回归处理而维护大量的历史数据。为此，需要设计一个简单的滤波器来递推估计差值序列的变化，进行相应的校

正。将这一新机制称为广播校正同步机制。需要指出的是，这里忽略了广播分组传播延时的差异给同步精度造成的影响。如果广播域覆盖半径约为 30m（ZigBee 标准定义的有效传输距离），最大的传播延时差异为 100ns，对于精度要求为毫秒或微秒级的同步算法，忽略传播延时差异是合理的。广播校正同步机制与其他同步补偿算法最大的区别在于：同步过程并非在某个时刻通过补偿一次完成，而是要经过一个动态调整的瞬态过程，进入稳态意味着实现了同步。本质上，广播校正同步机制主要利用了锁相环原理进行时钟频率锁定，最终实现了时钟同步。为了便于后面的论述，首先结合传统锁相环技术的锁频原理，介绍同步算法的机理。

在图 10.7 中，$h_1(k)$、$h_2(k)$ 分别表示广播分组中携带的参考时钟和任意节点的同步时钟，它们的差值 $e(k)$ 经过低通滤波器处理后，消除了高频噪声。为了方便设计，采用常用的比例积分简称 PI 控制器作为滤波器，控制信号 $v(k)$ 作为压控振荡器 VCO 的输入，K_0 是 VCO 的基准频率。不难看出，VCO 的输出频率 $f(k)$ 随着误差信号 $e(k)$ 动态地发生变化。$f(k)$ 经过零阶保持器和积分环节后转化为节点的同步时钟基于锁相环的时钟同步需要压控振荡器支持，追加额外的硬件是追求低成本节点实现所不期望的。为此，给出了下面的等价实现，它是全数字式，避免了对压控振荡器的依赖。

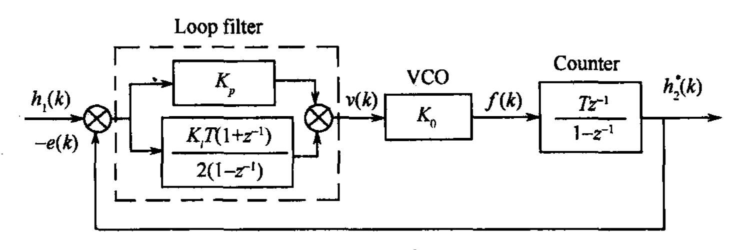


图 10.7　基于锁相环的时钟同步原理

此外，还有众多时钟同步协议和算法，感兴趣的读者可以参阅文献[15]～[18]。

10.3.5　同步算法性能比较

表 10.1 和表 10.2 为几种典型时间同步算法的性能及其参数的定量与定性比较。

表 10.1　同步算法性能定量比较

协 议	比较参数					
	精度/μs	Piggybacking	复杂度	收敛速度	网络规模/个	休眠模式
RBS	1.85 ± 1.28	N/A	高	N/A	2～20	是
Romer	3ms	是	低	N/A	未知	是
Mock et al	150	否	高	低	未知	否
Ganeriwal et al	16.9	否	低	未知	150～300	是
Ping	32	是	低	高	未知	否
PalChaudhuri et al	未知	未知	高	N/A	未知	是
Sichitiu et al	945	否	低	高	N/A	是
Time-Diffusion	100	否	高	高	200	是
Asynchronous diffusion	未知	否	高	高	200～400	是

表10.2　同步协议性能定性比较

协议	比较参数				
	精度	能量有效性	总体复杂度	可扩展性	容错性
RBS	高	高	高	好	否
Romer	低	高	低	差	否
Mock et al	高	低	低	N/A	是
Ganeriwal et al	高	一般	低	好	是
Ping	高	高	低	好	否
PalChaudhuri et al	未知	高	低	好	否
Sichitiu et al	高	高	低	N/A	是
Time-Diffusion	高	一般	高	好	是
Asynchronous diffusion	未知	低	高	N/A	是

10.4　时钟同步研究展望

目前,对无线传感器网络时间同步算法的研究已取得了很大进展,但是现有的时间同步算法还不够完善,在以下几个方面有待进一步研究:

(1)大规模节点时间同步。随着硬件技术的发展,传感器节点的成本将会逐渐降低,使今后进行大规模传感器节点的部署成为可能,现有的时间同步算法都是对中小规模的网络时间同步进行仿真和实验的,因此,时间同步算法在大规模网络中的应用是今后研究的方向之一。

(2)鲁棒性和容错性。目前提出的时钟同步算法基本上都是在实验室环境或开阔的室外环境下进行实现,传感器网络实际应用环境是人们难以接近的恶劣环境并存在诸多干扰因素。因此,时钟同步算法在实际应用中的鲁棒性和容错性仍值得研究。

(3)可变拓扑下时钟同步。下一代传感器网络包含大量移动传感节点,网络拓扑结构动态变化,如何解决动态拓扑下的时钟同步也需要进一步研究。

(4)性能评价模型。现有时钟同步算法之间的性能对比都是通过相同运行环境下的实验进行,因此,建立一个标准的性能评价模型也是一个值得研究的方向。

总之,无线传感器网络时钟同步是一个较新的研究领域,存在许多问题有待解决,值得广大研究人员关注并进一步研究。时间同步不仅要关注同步精度,还需要关注同步能耗、可扩展性和鲁棒性;经典的时钟同步协议侧重于同步精度和同步能耗需求,采用时钟漂移补偿、MAC层时戳技术以及双向报文交换来提高同步精度,充分利用无线传输的广播特性和捎带技术降低同步能耗;萤火虫同步和协作同步侧重于提高可扩展性和鲁棒性,适用于大规模无线传感器网络的应用。

参考文献

[1] Liskov B. Practical Uses of Synchronized Clocks in Distributed Systems[C]. Proc. Tenth Annual ACM Symposium on Principles of Distributed Computing, pp. 1-9, Aug. 1991.

[2] Ren FY, Dong SY, He T, etc. A time synchronization mechanism and algorithm based on phase lock loop[J]. Journal of Software, 2007,18(2):372 - 380. http://www.jos.org.cn/1000 - 9825/18/372.htm.

[3] Mills D L. Internet time synchronization: the network time protocol [A]. In Yang Z. and Marsland T. A. editors, Global States and Time in Distributed System[C]. IEEE Computer Society Press, 1994.

[4] Mannermaa J, Kalliomaki K, Mansten T, etc. Timing performance of various GPS receivers[A]. Proc. Joint Meeting Eur. Freq. Time Forum and IEEE Int. Freq. Control Symp[C]. April. 1999:287 - 290.

[5] Elson J, Girod L, Estrin D. Fine-grained network time synchronization using reference broadcasts[A]. Proceedings of the 5th Symposium Operating System Design and Implementation (OSDI 2002) [C]. Boston, MA, December 2002: 147 - 163.

[6] Su Ping. Delay Measurement Time Synchronization for Wireless Sensor Networks[R] IRB - TR - 03 - 013, Intel Research Berkeley, June, 2003.

[7] Miklos Maroti, Branislav Kusy, Gyula Simon. The Flooding Time Synchronization Protocol[A]. SenSys'04[C]. Baltimore, Maryland, USA, November, 2004:3 - 5.

[8] Ganeriwal S, Kumar R, Srivastava M B. Timing-Sync protocol for sensor networks[J] ACM press, 2003:138 - 149.

[9] Sichitiu M L, Veerarittiphan C. Simple, accurate time synchronization for wireless sensor networks[J]. IEEE Trans. on wireless communication and networking, 2003, (2):16 - 20.

[10] Bharath Sundararaman, Ugo Buy, Ajay D. Kshemkalyani Clock Synchronization for Wireless Sensor Networks: A Survey [J]. 2005, March 22.

[11] 程利娟. 无线传感器网络时间同步算法研究[D]. 西安:西北工业大学, 2007.

[12] Romer K. Time synchronization in ad hoc networks[C]. Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc'01), 2001: 173 - 182.

[13] Buck J, Buck E. Synchronous fireflies[J]. Scientific Amer, vol. 234, pp. 74 - 85, 1976.

[14] Ganeriwal S, Kumar R, Srivastava MB. Timing-Sync protocol for sensor networks[C]. In: Proc. of the 1st ACM Conf. on Embedded Networked Sensor Systems (SenSys). ACM Press, 2003. 138 - 149.

[15] Tulone D. Resource-Efficient Time Estimation for Wireless Sensor Networks[C]. Proc. DIALM - POMC Workshop on Foundations of Mobile Computing, S. Basagni and C. A. Phillips editors, pp. 52 - 59, Philadelphia, Pennsylvania, Oct. 2004. Available at hhttp://www.informatik.uni-trier.de//ley/db/conf/ dialm/dialm2004.html.

[16] Meier L, Blum P, Thiele L. Internal Synchronization of Drift-Constrained Clocks in Ad-Hoc Sensor Networks[C]. Proc. 5th ACM Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc '04), pp. 90 - 97, Roppongi Hills, Japan, May 2004.

[17] Van Greunen J, Rabaey J. Lightweight Time Synchronization for Sensor Networks[C]. Proc. 2nd ACM Int. Workshop on Wireless Sensor Networks and Applications (WSNA'03), pp. 11 - 19, San Diego, California, Sept. 2003.

[18] Hu A S, Servetto S D. Asymptotically Optimal Time Synchronization in Dense Sensor Networks[C]. Proc. 2nd ACM Int. Workshop on Wireless Sensor Networks and Applications (WSNA '03), pp. 1 - 10, San Diego, California, Sept. 2003.

第 11 章　无线传感器网络节点定位

节点定位是无线传感器网络的重要支撑技术之一，缺少位置信息的感知往往是没有意义的[1]。一方面，用于事件监测的网络需要知道节点在区域中的位置，以获得对监测区域的全局估计。例如，在战场环境中，通过对携带节点的单兵进行定位，便于为巷战提供邻近友军的清晰位置或进行战场精确搜救。另一方面，基于位置的路由协议、分簇和数据聚集算法、拓扑控制、覆盖控制等协议也需要知道节点的位置信息。

在实际应用中，大规模节点往往通过飞机或高射炮随机抛撒，节点的位置和相互关系不具有预知性。因此，在网络自组织过程中，需借助定位算法或安装辅助定位设备，如GPS 对节点进行定位，以充分发挥网络功能。随着无线传感器网络向节点数量多、铺设范围广、基础设施简单和硬件成本低的方向发展，如何在减少节点硬件组件、算法实现简单的同时获得相对准确的定位信息已成为主要研究的课题之一。

11.1　节点定位概述

现有定位算法根据定位过程中是否需要使用已知位置的锚节点或信标节点，分为绝对定位算法和相对定位算法。前者一般是在待测区域事先布置一定比例的锚节点，这些节点通过 GPS 或其他方法已获得自身绝对坐标，其余的未知节点通过与这些信标节点通信获得自身坐标。相对定位算法无需事先布置信标节点，通过算法制定的方案，选取一定数量的未知节点建立相对坐标，其余的节点通过节点之间的协作关系和消息传输获取自身在相对坐标系中的相对位置实现定位。相对定位算法无需锚节点和基础设施，硬件成本低，并且不会受复杂环境对远距离信号传输的影响，适合于对节点硬件、能耗以及环境适应性有很高要求的无线传感器网络应用。

节点定位算法的评价指标如下：

(1)定位精度。定位技术首要的评价指标是定位精度，一般用误差值与节点通信半径之比表示。不同类型的定位算法精度差异较大。基于距离的定位方法有较高的定位精度，但节点体积、功耗和成本也大。

(2)锚节点密度。锚节点是位置已知的节点，通常采用人工固定布置或 GPS 获得准确位置。人工部署的方式不仅受网络部署环境的限制，还严重制约了网络的可扩展性；采用 GPS 确定锚节点位置时，节点体积和代价增大。因此，锚节点密度也是评价定位算法性能的重要指标之一。

(3)鲁棒性和容错性。通常，定位系统和算法都需要比较理想的无线通信环境和可靠的网络节点设备。但在真实应用场合中，常会有诸如以下的问题。外界影响和节点硬件精度限制造成节点间点到点的距离或角度测量误差增大的问题；外界环境中存在严重

的多径传播、衰减、阴影、非视距(Non-Line-of-Sight,NLOS),通信盲点等问题;网络节点由于周围环境或自身原因(如电池耗尽、物理损伤)而出现失效的问题。由于环境、能耗和其他原因,人工维护或替换传感器节点或使用其他高精度的测量手段常常是十分困难或不可行的。因此,定位系统和算法的软、硬件必须具有很强的容错性和自适应性,能够通过自动调整或重构纠正错误、适应环境、减小各种误差的影响,以提高定位精度。

(4)能耗。能耗是对传感器网络的设计和实现影响最大的因素之一。由于传感器节点电池能量有限,因此在保证定位精度的前提下,与功耗密切相关的定位所需的计算量、通信开销、存储开销、时间复杂性、系统的附加设备能量消耗是一组关键性指标。

11.2　典型定位方法

根据定位机制可将现有无线传感器网络自身定位算法分为基于距离的(Range-based)和非基于距离的(Range-free)定位算法两类。基于距离的定位算法通过测量相邻节点之间的绝对距离或方位,并利用节点之间的实际距离来计算未知节点的位置;非基于距离的定位算法则无需距离和角度信息,仅根据网络连通性等信息实现定位。

11.2.1　基于距离的定位算法

基于距离的节点定位一般包括3个部分,即距离测定、位置计算和定位过程。

11.2.1.1　距离测定

基于测距的算法通过节点自身携带的测距功能直接测量两个节点之间的距离,比较重要的测距方法主要有到达时间(TOA)[1]、到达时间差(Time Difference On Arrival, TDOA)[2]和信号强度测距(RSSI)[3]或者到达角度(AoA)[4]。

TOA(Time of Arrival):该技术通过测量信号传播时间来测量距离。使用TOA技术最基本的定位系统是GPS,GPS系统需要昂贵、高性能的电子设备来精确同步卫星时钟。因节点硬件尺寸、价格和功耗限制,GPS和其他TOA技术无法广泛应用于无线传感器网络。

TDOA测距技术被广泛应用于节点定位方案中。通过记录两种不同信号(常使用RF和超声波)到达时间差,基于已知信号传播速度,把时间转化为距离。已有多种定位算法[5-7]使用TDOA实现测距,但该技术受限于超声波传播距离有限(超声波信号通常传播距离仅为20英尺~30英尺,因而网络需要密集部署)和NLOS(Non-Line-Of-Sight)问题对超声波信号的传播影响。虽然已有发现并减轻NLOS影响的技术,但都需要大量计算和通信开销,不适用于低功耗的无线传感器网络应用中。TDOA测距技术如图11.1所示。

RSSI(Received Signal Strength Indicator):已知发射功率,在接收节点测量接收功率,计算传播损耗,使用理论或是经验的信号传播模型将传播损耗转化为距离,该技术主要使用RF信号。因传感器节点具有无线通信能力,故RSSI是一种低功率、廉价的测距方式,RADAR、SpotON等许多项目中使用了该技术。其主要误差来源是环境影响所造成的信号传播模型的建模复杂性、反射、多径传播、NLOS以及天线增益等问题,这些都会对相同的距离产生显著不同的传播损耗。通常,将其看为一种粗糙的测距技术,它可能产生50%的测距误差。

AoA(Angle of Arrival):该技术是估算邻节点发送信号方向,可通过天线阵列或多个

接收器来实现,除定位外,还能提供方向信息,如 MIT 的 The Cricket Compass 等项目中都使用 AoA 技术。AoA 测距与定位原理如图 11.2 所示。

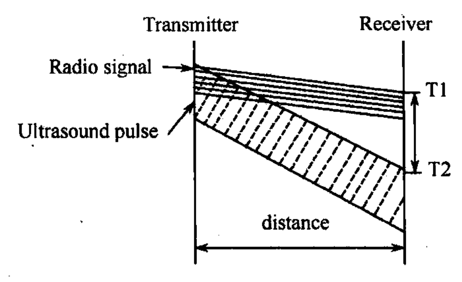


图 11.1 TDOA 测距技术示意图

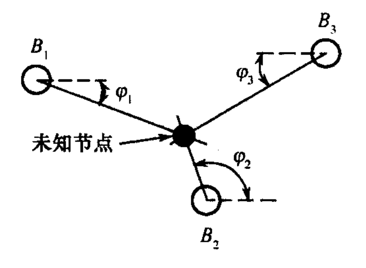


图 11.2 AoA 测距与定位原理

11.2.1.2 位置计算

在获取上述距离值之后,节点需要通过位置计算的方法计算得到坐标值。现有的算法一般采用三边测量法(图 11.3)、三角测量法和极大似然法计算坐标。

对于图 11.3 所示的三边测量法,在未知节点获得 3 个以上的信标节点距离值之后,就可通过式(11.1)、式(11.2)和式(11.3)计算自身坐标。

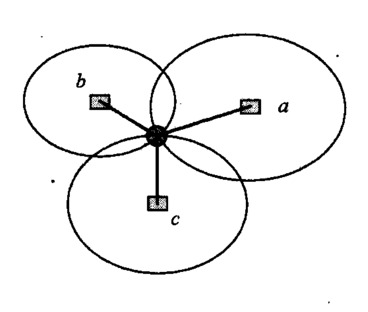


图 11.3 三边测量法示意图

$$\begin{cases} \sqrt{(x-x_a)^2+(y-y_a)^2}=d_a \\ \sqrt{(x-x_b)^2+(y-y_b)^2}=d_b \\ \sqrt{(x-x_c)^2+(y-y_c)^2}=d_c \end{cases} \tag{11.1}$$

式中:(x_a, y_a)、(x_b, y_b)、(x_c, y_c)分别是 3 个信标节点的坐标;d_a、d_b、d_c 是未知节点到 3 个信标节点的距离。

式(11.1)经过线性化,可得线性方程式

$$\boldsymbol{AX}+\boldsymbol{N}=\boldsymbol{B} \tag{11.2}$$

$$\boldsymbol{A}=\begin{bmatrix} 2(x_a-x_c) & 2(y_a-y_c) \\ 2(x_b-x_c) & 2(y_b-y_c) \end{bmatrix},\quad \boldsymbol{B}=\begin{bmatrix} x_a^2-x_c^2+y_a^2-y_c^2+d_c^2-d_a^2 \\ x_b^2-x_c^2+y_b^2-y_c^2+d_c^2-d_b^2 \end{bmatrix},\quad \boldsymbol{X}=\begin{bmatrix} x \\ y \end{bmatrix}$$

使用标准的最小均方差估计可得未知节点的坐标为

$$\boldsymbol{X}=(\boldsymbol{AA}^{\mathrm{T}})^{-1}\boldsymbol{A}^{\mathrm{T}}b \tag{11.3}$$

式(11.2)中的 N 是由于存在测距误差引入的参数,它是根据测距误差的分布形式存在的一个随机误差矢量。如果未知节点测得的到信标节点的距离值大于 3 个,则可以加入式(11.1)中,进行更精确的计算。

三角测量法与三边测量法类似,通过获取相对 3 个信标节点的角度值,计算得到图 11.3 中 3 个圆的半径,再经三边测量法计算坐标。三角测量定位方法也称为 AoA 定位方法或方位测量定位方法,该方法通过未知节点接收器天线或天线阵列测出锚节点发射电波的入射角,从而构成从目标节点到锚节点的径向线,即方位线。在二维平面中,利用两个或更多锚节点的 AoA 测量值,按照 AoA 定位算法确定多条方位线的交点,即可计算出未知节点的估计位置。三角测量法定位原理如图 11.4 所示。

假设未知节点 A 的坐标为(x_0, y_0),分别测得锚节点 B、锚节点 C 的信号到达角为 θ_1 和 θ_2,则

$$\tan\theta_i = \frac{x_0 - x_i}{y_0 - y_i} \quad (i = 1,2) \tag{11.4}$$

三边测量法和三角测量法由于涉及大量的矩阵运算和最小二乘的运算,计算量较大。针对这种情况,加州大学洛杉矶分校的 Andreas Savvides 等人提出的 n-hop Multi-Lateration Primitive 定位算法中提出的最大最小值法[8]通过简单的折线运算估计未知节点的位置,如图 11.5 所示。

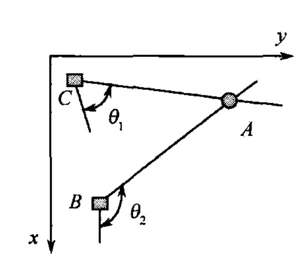


图 11.4　三角测量法示意图

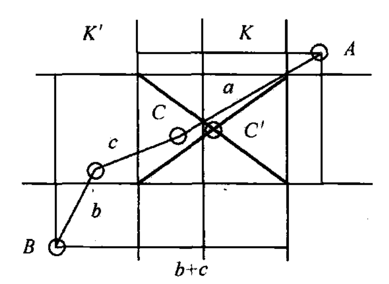


图 11.5　最大最小值法示意图

图 11.5 中,A 点和 B 点为信标节点,C 点为未知节点。在获得 C 点到 A 点和 B 点的折线距离 a、b、c 之后,在三角形 ACK 中,利用斜边 AC 的长度 a 代替直角边 AK 的长度,从而 K 点移动到 K′点,B 点类似,从而有:

$$A\text{ 点} \Rightarrow \begin{cases} x_c = x_a - a \\ y_c = y_a - a \end{cases} \tag{11.5}$$

$$B\text{ 点} \Rightarrow \begin{cases} x'_c = x_b + (b + c) \\ y'_c = y_b + (b + c) \end{cases} \tag{11.6}$$

以($x_c - x'_c$)和($y_c - y'_c$)为边长可得图 11.5 中实线画出的矩形区域,以矩形区域的质心 C′作为 C 点的估计位置,可得

$$\begin{cases} x = \dfrac{x_c + x'_c}{2} = \dfrac{x_a + x_b + (b + c - a)}{2} \\ y = \dfrac{y_c + y'_c}{2} = \dfrac{y_a + y_b + (b + c - a)}{2} \end{cases} \tag{11.7}$$

最大最小值法估计得到的坐标值由于是用矩形区域的质心代替实际位置,若测得的距离值本身就存在较大误差,那么得出的结果没有三边定位精确,在一些要求精度不是很严格的情况或者是结果经过求精之后,可以满足需要。

极大似然估计法(Maximum Likelihood Estimation)原理:已知 n 个节点的坐标分别为 $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$,它们到节点 D 的距离分别为 $d_1, d_2, \cdots, d_n$,假设节点 D 的坐标为 (x, y),如图 11.6 所示。

则有

$$\begin{cases}(x_1-x)^2+(y_1-y)^2=d_1^2\\ \vdots\\ (x_n-x)^2+(y_n-y)^2=d_n^2\end{cases} \tag{11.8}$$

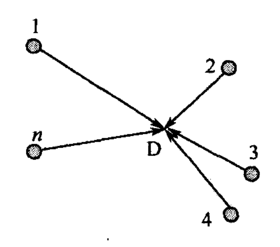


图 11.6　极大似然估计法

从第一个方程开始分别减去最后一个方程，得

$$\begin{cases}x_1^2-x_n^2-2(x_1-x_n)x+y_1^2-y_n^2-2(y_1-y_n)y=d_1^2-d_n^2\\ \vdots\\ x_{n-1}^2-x_n^2-2(x_{n-1}-x_n)+y_{n-1}^2-2(y_{n-1}-y_n)y=d_{n-1}^2-d_n^2\end{cases} \tag{11.9}$$

式(11.9)中的线性方程为

$$AX=b$$

其中

$$A=\begin{bmatrix}2(x_1-x_n) & 2(y_1-y_n)\\ \vdots & \\ 2(x_{n-1}-x_n) & 2(y_{n-1}-y_n)\end{bmatrix},b=\begin{bmatrix}x_1^2-x_n^2+y_1^2-y_n^2+d_n^2-d_1^2\\ \vdots\\ x_{n-1}^2-x_n^2+y_{n-1}^2-y_n^2+d_n^2-d_{n-1}^2\end{bmatrix},X=\begin{bmatrix}x\\ y\end{bmatrix}$$

使用标准的最小均方差估计法，可得节点 D 的坐标为

$$\hat{X}=(A^TA)^{-1}A^Tb \tag{11.10}$$

11.2.1.3　定位过程

不同算法根据上面两步获得的有限的距离值和部分节点的坐标，计算其余未知节点的机制。由于各种算法采取的策略不同，各种性能参数的区别主要由这一步决定。在分析定位算法时，一般要针对具体情况综合考虑上述 3 个方面来考察算法性能。

1. SPA 算法

瑞士洛桑联邦工业大学的 Srdjan Capkun 等人最早针对没有基础设施的移动无线自组网，提出 SPA(Self-Positioning Algorithm)算法[9]。它以网络中节点密度最大的地方选取一个参考点作为全局相对坐标系的原点，其余每个节点分别通过测距功能测得邻节点之间的距离值，如图 11.7 所示。图中，实线表示二者距离可测得，虚线表示二者不是邻节点。每个节点在邻节点中选取两个点 A、B，选取原则是这两个点本身也是邻节点，并且 3 个点不在同一直线上。以直线 OA 作为 x 轴，以 B 点在 OA 上的投影 B_xB 为 y 轴正方向建立局部相对坐标系。所有的局部坐标系建立完成后，相邻的坐标系通过坐标变换实现坐标统一，最终所有节点都变换成以选取的参考点为原点的坐标系实现定位。由于每个节点都要参与多次的坐标变换，计算量和通信开销都非常大。

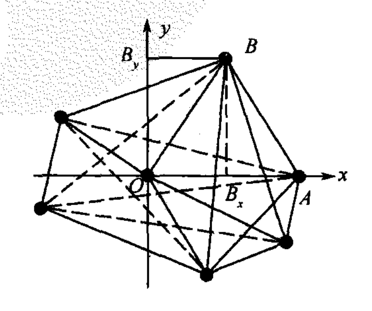


图 11.7　SPA 算法示意图

SPA 算法开始是针对无线自组网提出的，未考虑功耗问题，但是用于无线传感器网络当中，这种通信开销和节点数量呈指数比上升的算法需要根据实际情况进行改进。

2. 聚类SPA算法

美国仁斯利尔理工学院Rajagopal Iyengar等人提出的聚类SPA(Clustering-Based Self-Positioning Algorithm)算法[10]是针对SPA算法通信量过大而提出的改进算法。首先通过运行随机的定时器选取网络中的主节点,主节点一跳范围内的其他节点成为它的从节点。每个主节点使用SPA算法中相似的方法建立局部相对坐标系,并计算得到其余从节点的局部坐标。完成第一步之后,相邻的局部坐标系依据ID号由大到小的原则进行坐标变换,最终以ID号最小的主节点为原点建立相对坐标系,从而实现定位。由于算法以节点簇为单位进行坐标变换,计算量和通信量相对SPA算法来说都得到大幅度减少,基本与节点个数呈线性比。该算法由于簇之间变换要求拓扑结构比较规则,通信无障碍,所以在地形复杂、节点之间通信容易产生冲突的环境下,定位效果不是很好,节点覆盖率比较低。

3. Map-growing算法

美国密苏里大学哥伦比亚分校的Xiaoli Li等人提出的Map-growing算法[11]同样基于测距,其基本思想是通过递归算法,重复进行三边定位实现节点坐标获取。首先在区域节点密度比较大的地方选取一个点O作为相对坐标系的坐标原点,如图11.8所示。在其邻节点里面选取两个点,选取原则是三点能构成一个良好三角形(3个内角都大于30°)。以其中一个点A作为x轴,另外一个点B确定y轴正方向建立坐标系,B点坐标通过式(11.12)求得,即

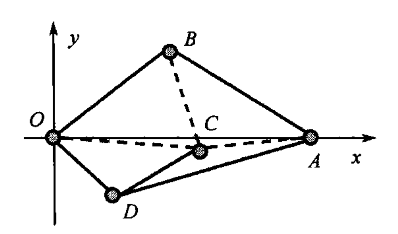


图11.8　Map-growing算法示意图

$$\theta = \arccos \frac{d_{ab} + d_{ca} - d_{ab}}{2d_{ca}d_{ab}} \tag{11.11}$$

$$\begin{cases} x_b = d_{ab} \times \cos\theta \\ y_b = d_{ab} \times \sin\theta \end{cases} \tag{11.12}$$

同时与O、A、B三个点为邻节点的未知节点C首先通过三边定位法计算得到自身的相对坐标,计算完成后,也将自身的坐标广播,与B点不是邻节点的D点收到C点发来的坐标消息后,通过O、A、C三个点实现定位并发布消息,重复运行此步,直到所有能计算得到坐标的未知节点都得到定位。

该算法实现简单,只需首先确定3个点建立相对坐标系就可实现区域大部分节点的定位。由于不断升级新的未知节点参与到坐标定位中来,该算法对拓扑结构适应性很强,节点覆盖率高。Map-growing算法是局部定位算法,对于任意一个节点来说,只要其邻节点有3个能确定坐标,它自身的坐标就能确定,并不需要考虑整体布局如何,只要局部区域满足要求就能实现定位,适合于节点密度大、地形相对复杂的区域使用。但是该算法使用本身就是经过计算得到坐标的点协助定位会造成误差累计,一旦测距误差比较大时,距离3个选取的参考点较远的边缘区域节点计算得到的坐标误差就会很大,精度有待提高。

4. LDP算法

美国马里兰大学的Adel Youssef等人提出的LDP(Local Discovery Position)算法[12]同样是一种基于三边定位的相对定位算法。该算法分为以下3个阶段:

(1)在网络中选取节点作为网关节点建立节点簇,簇半径参数 k 和网关节点的数量依据节点连通度的情况取值。节点经过测距获得邻节点的距离值,大于一跳的节点记录每个网关节点的最小跳数估计距离。

(2)每个网关节点采取 Map-growing 算法类似的方法建立相对坐标系,并通过三边定位的方式向外扩展,收到两个网关节点信息的未知节点选取距离近的网关节点作为坐标原点计算坐标。

(3)每个网关节点建立的坐标系统相互转换,构成一个统一的全局坐标。

该算法在递归调用三边定位的基础上加入了分簇的思想,使得靠近边缘的节点不再由于远离坐标原点而增加误差,每个点都以距离自己比较近的网关节点建立自己的坐标,从而减少了误差累计的影响,提高了定位的精度。但是不同网关节点之间要进行变换统一坐标,增加了计算量和通信量,并且和 Map - growing 算法一样,需要在节点密度较高的区域才能获得好的定位效果。

5. GFF 算法

法国巴黎大学的 Farid Benbadis 等人提出的 GFF (GPS Free Free)算法[13]是一种 Range-free 算法。该算法采用和 DV-hop 类似的距离矢量路由思想,通过两点之间的最小跳数估算这两个点的距离,如图 11.9 所示。

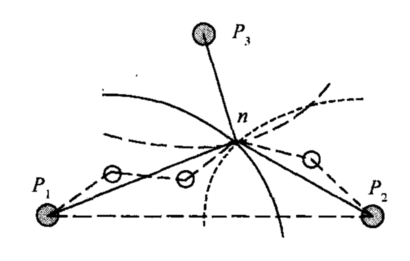


图 11.9　GFF 算法示意图

图 11.9 中构建相对坐标系的 P_1,P_2,P_3 是位于网络边缘的点。首先原点 P_1 发布一个 DDP(Distance Discovery Packet)包,包括坐标(0, 0)和自身的 ID 号,其余节点转发消息,每次转发都将跳数加 1,并且每个节点对同一个数据包都只接收最小跳数并转发,抛弃跳数大于节点记录跳数的数据包。这样,当 P_2 接收到这个包的时候就以最小跳数 d 确定 x 轴。同理,它再向 P_3 发送包含自身 ID 和坐标值(d,0)的 DDP 包,P_3 收到这两个 DDP 包之后就能根据三者之间的距离确定 y 轴正向,同时,其他的节点 n 也知道了 P_1,P_2,P_3 三点之间的距离和每个点到这 3 个点的跳数。通过三边定位,每个节点就能计算得到以跳数表示的相对坐标。

如图 11.9 中所示,以跳数代替直线距离会存在误差,且跳数越多的点,估算的距离值就越不准确。该算法优势在于无需节点有测距功能,硬件成本低,并且实现简单,计算量和通信量较小,由于该算法始终都只有 3 个节点充当锚节点,在节点密度较小的区域会出现无法与锚节点通信的失效节点,定位精度下降严重,只有在节点密度高的环境下能很好定位。

6. MDS-MAP 算法

美国密苏里大学哥伦比亚分校的 Yi Shang 等人提出的 MDS-MAP(Multi Dimensional Scaling MAP)算法[14]分别可以在 Range-Based 和 Range-Free 两种状态下运行,并且根据需要该算法可以分别实现相对定位和绝对定位,在 range-free 的情况下,节点之间仅仅依靠连通度信息建立相对坐标系统。

MDS 是多维定标分析,它是一种源自心理测量学和精神物理学的数据分析技术,主要思想是通过降维,在低维数空间中可以体现原来在高维数时的某些特征,从而能在低维数条件下进行处理。对于任意的两个点,它们在原来的高维空间中的距离与将维数约简

后的低维空间(一维或者是二维)中的距离相同,从而在低维空间可以重建两点在原来高维空间中的距离特征,体现高维空间的误差信息。

MDS-MAP 算法将多维定标分析方法运用到节点定位中,通过建立最短距离的相似矩阵确定节点位置,算法主要分为以下 3 步:

(1)从全局网络部署出发,计算所有节点间的最短路径,建立最短路径距离矩阵。如果节点具备测距功能,那么节点间距就是所测距离,如果不基于测距,只知道节点之间的连通度信息,就设节点之间的距离统一为 1。然后使用最短路径算法生成节点间距矩阵。

(2)对距离矩阵直接使用 MDS 标准算法,将其中具有最大特征值的 2 个或是 3 个距离矩阵保留下来,建立二维或是三维的相对坐标系统。

(3)在拥有足够的已知绝对位置信息的锚节点条件下,将建立的相对坐标系转换为绝对坐标系。

MDS-MAP 算法适用于节点密度较大的区域,能基本实现 100% 的节点定位,但是由于该算法涉及很多的矩阵复杂运算,当节点数目较多时,算法复杂度为 $O(n^3)$,计算量大,节点耗能也比较大,并且该算法是集中式的,无法应用于需要节点分别计算坐标的区域。当节点连通度较小的时候,算法测距误差急剧增大,定位覆盖率不高,需要对计算过程有所简化。

11.2.2　非基于距离的定位算法

无需测距的算法不需要节点自身的测距设备,通过跳数或是其他信息估计自身到选定的信标节点的距离值。由于是估计得到的数值,相对于基于测距的算法获得的距离值误差偏大。常用的定位算法有质心法[15]、凸规划[16]、DV-Hop 算法[17]、Amorphous 算法[18]、MDS-MAP[19]和 APIT[20]算法等。

1. 质心法

文献[15]提出了一种无需测距的粗粒度算法,如图 11.10 所示。此算法只需利用锚节点的坐标(x_i,y_i)即可估算未知节点的坐标,当未知节点接收到锚节点的位置信息后,用如下公式计算未知节点位置:

$$(x,y) = \left(\sum x_i/N, \sum y_i/N\right) \tag{11.13}$$

该算法的最大优点在于算法不需要信标节点和未知节点间的协调,因此算法简单且容易实现。但是,算法假设节点均具有理想的球形无线信号传播模型,而实际上并非如此;而且算法的精度与信标节点的密度及分布有很大关系,密度越大、分布越均匀,定位精度越高;而且,对于位于传感器场边缘的未知节点其定位误差很大。

2. APIT 算法

APIT 算法的基本思想:未知节点监听自己附近锚节点的信息,然后从这些锚节点组成的集合中任意选取 3 个节点。假设集合中有 n 个节点,那么共有 C_n^3 种不同的选取方法,确定 C_n^3 个不同的三角形,逐一测试未知节点是否位于每个三角形内部,直至穷尽所有的组合。最后,计算包含未知节点所有三角形的重叠区域,将重叠区域的质心作为未知节点的位置。如图 11.11 所示,阴影部分区域是包含未知节点的所有三角形的重叠区域,黑色指示的质心位置作为未知节点的位置。

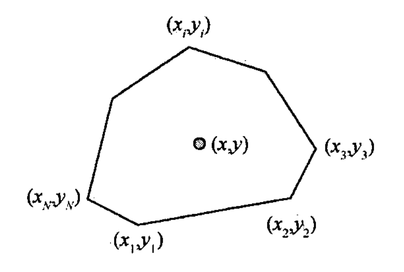


图 11.10　质心法示意图

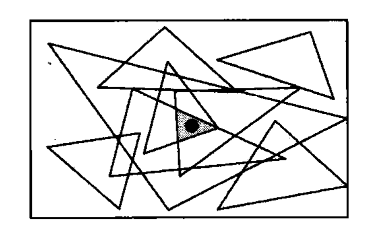


图 11.11　APIT 定位算法原理

APIT 算法的理论基础是最佳三角形内点测试法(Perfect Point-In-Triangulation Test, PIT 测试),PIT 测试原理如图 11.12 所示。假如存在一个方向,沿着这个方向未知节点 M 会同时远离或接近三角形的 3 个端点 A、B、C,则 M 位于 $\triangle ABC$ 外;否则,M 位于 $\triangle ABC$ 内。

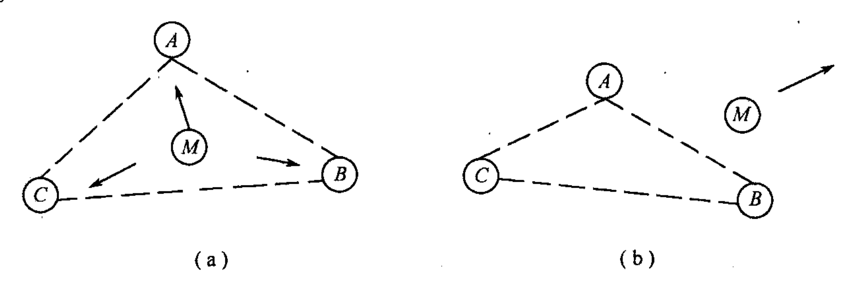


图 11.12　PIT 原理示意图

为了在静态网络中执行 PIT 测试,APIT 测试(Approximate PIT Test)应运而生:假设节点 M 的邻节点没有同时远离/靠近 3 个锚节点 A、B、C,那么,M 就在 $\triangle ABC$ 内;否则,M 在 $\triangle ABC$ 外。APIT 算法利用传感器网络较高的节点密度来模拟节点移动,利用无线信号的传播特性来判断是否远离或靠近锚节点。通常在给定方向上,一个节点距锚节点越远、接收信号强度越弱,并通过信息交换来判断与某一锚节点的远近,以此来仿效 PIT 中的节点移动。

APIT 定位原理如图 11.13(a),节点 M 通过与邻节点 1 交换信息,得知自身若运动至节点 1,将远离锚节点 B 和 C,但会接近锚节点 A。邻节点 2、3 和 4 的通信及判断过程类似,最终确定自身位于 $\triangle ABC$ 中。在图 11.13(b)中,通过信息交换节点 M 可知:邻节点 3 将同时远离锚节点 A、B 和 C,故判断自身不在 $\triangle ABC$ 中。

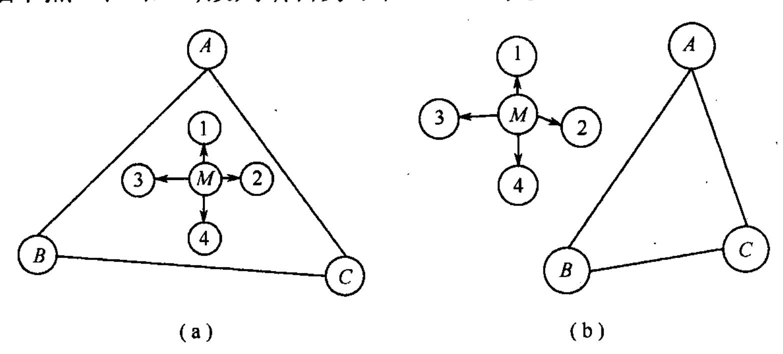


图 11.13　APIT 定位原理示意图

3. DV-Hop 算法

Rutgers 大学的 Dragos Niculescu 等[17]利用距离矢量路由和 GPS 的思想提出了一系列分布式定位算法，合称为 APS(Ad hoc Positioning System)，DV-Hop(Distance Vector-Hop)算法是其中之一。

因传感器节点通信距离有限，通常通过多跳路由的方式传送数据，节点本身只与邻节点交换信息。DV-Hop 算法正是充分利用了传感器网络的这一特性。在距离矢量定位机制中，普通节点首先计算与信标节点的最小跳数，然后根据信标节点估算到的平均每跳的距离，利用最小跳数乘以平均每跳距离，得到目标节点与锚节点之间的估计距离。虽然目标节点无线通信半径内的参考节点数量不多，但是采用上述方法可以获得通信范围外多个参考节点的估计距离，利用大量的冗余信息实现比较精确的节点定位。

该算法的实现大致分为3个阶段。在第一阶段中，网络中的各个节点采用典型的距离矢量交换协议，使网络中所有节点获得距锚节点的跳数。第二阶段中，在获得到其他锚节点位置和相隔跳数后，锚节点计算网络平均每跳距离，然后将其作为一个校正值(correction)广播至网络中，目标节点根据其接收到的第一个校正值(对该校正值立即转发，而丢弃之后收到的校正值)，以及第一阶段中得到的距各个锚节点跳数来近似计算到各个参考节点的距离。第三阶段中，当目标节点获得与3个或更多锚节点的距离之后，利用三边测量法或其变换形式，也即利用 GPS 定位原理，将 GPS 的四维(三维坐标加时钟同步)求解缩减到二维求解，来估计节点的二维坐标值，实现节点的定位。

DV-Hop 算法没有直接地进行距离的测量，仅根据网络的连通性和距离矢量信息的交换，巧妙地将其转化为近似的距离测量，因此，该算法不需要装备昂贵的测距单元，在各向同性的网络中性能良好。

4. DV-Distance 算法

DV-Distance 算法和 DV-Hop 算法很类似。略微不同的地方有以下两点：

(1)在距离矢量报文交换阶段，交换的不是节点间的跳数，而是采用 RSSI、ToA 等方法得到的估计距离之和。

(2)由于用节点间估计距离之和来代替两个节点间的直线距离，有过估计的倾向，所以应该利用 DV-Hop 计算校正值的一样方法来得到直线距离与折线距离和的大致比例。除此之外的其他步骤，DV-Distance 算法和 DV-Hop 算法相同。

11.3　基于时间差的节点定位方法

11.3.1　网络模型与定位算法

为便于表述，以下将位置已知的节点称为锚节点，待定位的节点称为目标节点。假设传感器节点随机分布在二维监测区域中，3个锚节点 A、B 与 C 置于监测区域的外围，坐标分别为(x_a,y_a)、(x_b,y_b)和(x_c,y_c)，目标节点坐标为(x,y)。3个基站不共线，每个锚节点可以和目标节点进行单跳 RF 通信，网络模型如图 11.14 所示。

此外，锚节点之间以及锚节点与目标节点之间无时间同步的要求。如果待定位的区域很大，3个锚节点无法覆盖，可将区域划分成若干个小区域，分别对每个区域内的节点

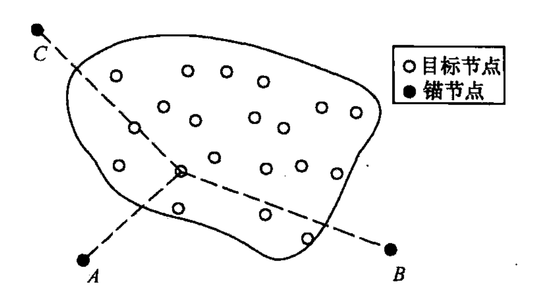


图 11.14　网络模型

进行定位。

设锚节点 A 为主站，负责向锚节点 B、C 和目标节点 S 发送初始定位信号，其格式如表 11.1 所列。锚节点 B、C 与目标节点 S 均有局部时钟，用来记录定位信号到达自身的时刻。节点 S 根据数据包中的"锚节点名称"可判断是何锚节点发送的定位信号。

表 11.1　定位信号格式

起始位	锚节点名称	锚节点坐标	节点延时	校验位	停止位

锚节点 B、C 与目标节点 S 接收到锚节点 A 的定位信号的时刻分别为 t_b，t_c 和 t_1；在节点 B 和 C 分别产生 Δt_b 和 Δt_c 延时后，定位信号被转发至节点 S；目标节点 S 分别在 t_2 和 t_3 时刻接收到这两个锚节点的定位信号，定位信号传播过程如图 11.15 所示。

其中：t_b、Δt_b 由锚节点 B 的局部时钟确定；t_c、Δt_c 由锚节点 C 的局部时钟确定；t_1、t_2 和 t_3 由目标节点 S 的局部时钟确定。换言之，锚节点之间以及锚节点与目标节点之间无需时钟同步。

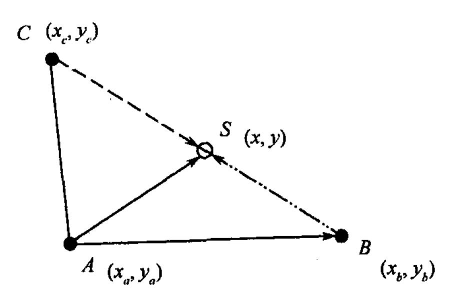


图 11.15　定位信号传播过程

由图 11.15 可知

$$\frac{d_{AB}}{v} + \Delta t_b + \frac{d_{BS}}{v} - \frac{d_{AS}}{v} = t_2 - t_1 \tag{11.14}$$

$$\frac{d_{AC}}{v} + \Delta t_c + \frac{d_{CS}}{v} - \frac{d_{AS}}{v} = t_3 - t_1 \tag{11.15}$$

式中：$d_{AB} = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$，为锚节点 A 与 B 之间的距离；$d_{AC} = \sqrt{(x_a - x_c)^2 + (y_a - y_c)^2}$，为锚节点 A 与 C 之间的距离；v 为 RF 信号的传播速度。

对式(11.14)、式(11.15)进行变换，得

$$d_{BS}=d_{AS}+k_1 \tag{11.16}$$

$$d_{CS}=d_{AS}+k_2 \tag{11.17}$$

式中

$$k_1=v(t_2-t_1)-v\Delta t_b-d_{AB}=v[(t_2-t_1)-\Delta t_b]-d_{AB}$$

$$k_2=v(t_3-t_1)-v\Delta t_c-d_{AC}=v[(t_3-t_1)-\Delta t_c]-d_{AC}$$

据此，建立如下方程组：

$$\begin{cases}(x-x_a)^2+(y-y_a)^2=d_{AS}^2\\(x-x_b)^2+(y-y_b)^2=(d_{AS}+k_1)^2\\(x-x_c)^2+(y-y_c)^2=(d_{AS}+k_2)^2\end{cases} \tag{11.18}$$

为计算方便，以锚节点 A 为坐标原点，并使锚节点 B 与之共线，以减轻目标节点 S 的计算负担，即 $x_a=y_a=y_b=0, x_b=x_1, x_c=x_2$ 且 $y_c=y_2$，则方程组(11.18)简化为

$$x^2+y^2=d_{AS}^2 \tag{11.19}$$

$$x^2-2xx_1+x_1^2+y^2=d_{AS}^2+2d_{AS}k_1+k_1^2 \tag{11.20}$$

$$x^2-2xx_2+x_2^2+y^2-2yy_2+y_2^2=d_{AS}^2+2d_{AS}k_2+k_2^2 \tag{11.21}$$

式(11.20)减去式(11.19)，得

$$2xx_1=-2d_{AS}k_1-k_1^2+x_1^2 \tag{11.22}$$

式(11.21)减去式(11.19)，得

$$2xx_2+2yy_2=-2d_{AS}k_2-k_2^2+x_2^2+y_2^2 \tag{11.23}$$

根据式(11.22)与式(11.23)可知

$$\begin{cases}x=\dfrac{-2k_1d_{AS}-k_1^2+x_1^2}{2x_1}\\y=\dfrac{2d_{AS}(k_1x_2-k_2x_1)+k_1^2x_2-k_2^2x_1+x_1x_2^2-x_1^2x_2+x_1y_2^2}{2x_1y_2}\end{cases} \tag{11.24}$$

将上述 x 与 y 代入式(11.19)，经整理得

$$\alpha d_{AS}^2+\beta d_{AS}+\gamma=0 \tag{11.25}$$

特别地，当3个锚节点呈等边直角三角形布置，即 $x_2=0, x_1=y_2=R$（R 为直角边长）时，则 $\alpha=4(k_1^2+k_2^2-R^2)$，$\beta=4[k_1(k_1^2-R^2)+k_2(k_2^2-R^2)]$，$\gamma=(k_1^2-R^2)^2+(k_2^2-R^2)^2$。显然，$\gamma\geqslant0$。由于 x 与 y 均为 d_{AS}的函数，研究式(11.25)的一元二次方程根的分布情况，可知目标节点坐标分布。下面分情形讨论该一元二次方程根的分布：

(1)当 $\gamma=0$ 时，有 $k_1=k_2=R$，则 β 亦为0，方程(11.25)无正实根。

(2)当 $\gamma>0$ 且 $\alpha=0$ 时，$d_{AS}=\dfrac{-\gamma}{\beta}$。若此时 $\beta<0$，则方程(11.25)有唯一正实根。

(3)当 $\gamma>0$ 且 $\alpha<0$ 时，抛物线 $Y=\alpha X^2+\beta X+\gamma$ 开口向下，在 Y 轴上的截距为正，则方程(11.25)有两个异号的实根，其正实根为 $d_{AS}=\dfrac{-\beta-\sqrt{\beta^2-4\alpha\gamma}}{2\alpha}$。

(4)当 $\gamma>0$ 且 $\alpha>0$ 时,抛物线 $Y=\alpha X^2+\beta X+\gamma$ 开口向上,在 Y 轴上的截距为正。

若 $\beta^2-4\alpha\gamma<0$,抛物线与 X 轴无交点,方程(11.25)无实根;

若 $\beta^2-4\alpha\gamma>0$,抛物线与 X 轴有两个交点,方程(11.25)有两个符号相同的异实根;

若 $\beta^2-4\alpha\gamma=0$,抛物线与 X 轴有且只有一个交点,方程(11.25)有两重实根,为 $d_{AS}=\dfrac{-\beta}{2\alpha}$。

考虑到在实际定位过程中,锚节点 A 与目标节点 S 之间的物理距离为正实数,故满足下列条件之一即可完成对 S 的位置估计:

(1)$\alpha=0,\beta<0,\gamma>0$。

(2)$\alpha<0,\gamma>0$。

(3)$\alpha>0,\beta<0,\gamma>0$ 且 $\beta^2-4\alpha\gamma=0$。

11.3.2　定位误差分析

一般情况下,总能满足 $\alpha<0$ 且 $\gamma>0$。即选择合适的锚节点的位置,总可以对节点进行定位,但坐标的解算精度受 k_1 和 k_2 影响。从 k_1 与 k_2 的表达式来看,其精度由锚节点 B、C 和目标节点 S 局部时钟的测量精度决定。根据中心极限定理[5],当测量次数足够多时,k_1、k_2 满足 $N(0,\sigma_1^2)$ 和 $N(0,\sigma_2^2)$ 分布,且相互独立。据此,利用 $k_1^2/R^2\approx0$、$k_2^2/R^2\approx0$ 和 $k_1k_2/R^2\approx0$ 可得以下近似结果:

$$\begin{cases}d_{AS}\approx\dfrac{-(k_1+k_2)+\sqrt{(k_1+k_2)^2+2R^2}}{2}\\[2ex] x\approx\dfrac{R}{2}+\dfrac{k_1}{2}\left(\dfrac{k_2}{R}-\sqrt{2}\right)\\[2ex] y\approx\dfrac{R}{2}+\dfrac{k_2}{2}\left(\dfrac{k_1}{R}-\sqrt{2}\right)\end{cases}\tag{11.26}$$

研究 x 与 y 的方差可知:$D(x)=Ex^2-E^2x=\dfrac{\sigma_1^2}{2}\left(\dfrac{\sigma_2^2}{2R^2}+1\right)$,$D(y)=Ey^2-E^2y=\dfrac{\sigma_2^2}{2}\left(\dfrac{\sigma_1^2}{2R^2}+1\right)$。从 $D(x)$ 和 $D(y)$ 的表达形式来看,当 k_1、k_2 不存在测量误差,即 $\sigma_1^2=\sigma_2^2=0$ 时,位置估计亦不存在误差。当等边直角三角形的边长 $R\to\infty$ 时,$D(x)=\dfrac{\sigma_1^2}{2}$,$D(y)=\dfrac{\sigma_2^2}{2}$。这就意味着在布置锚节点时,可通过增加锚节点间的距离来提高定位精度。

11.3.3　定位试验

利用无线传感器网络测试床验证上述定位算法的有效性,其中锚节点与目标节点的配置如表 11.2 所列。锚节点采用 8 位 MCU,目标节点由于承担定位算法和与 PC 机的通信,采用 16 位 ARM 核的 MCU;两种类型的节点均采用 3 节 1.5V 的 AA 电池供电。

锚节点与目标节点的布置如图 11.16 所示,3 个锚节点呈等边直角三角形放置,待定位的目标节点放置在 3 个锚节点的通信范围内,以避免隐终端和暴露终端问题。在试验

过程中，固定目标节点的位置，使 $x=3$，$y=4$，改变三角形的边长 R，验证定位精度与 R 的关系。

表 11.2　锚节点与目标节点的配置

配 置	锚 节 点	目标节点
MCU	ADu832	LPC2210
射频模块	nRF905	nRF905
通信距离/m	≤200	≤200
电源	AA 型 1.5V×3	AA 型 1.5V×3
接口	无	以网口与 PC 连接

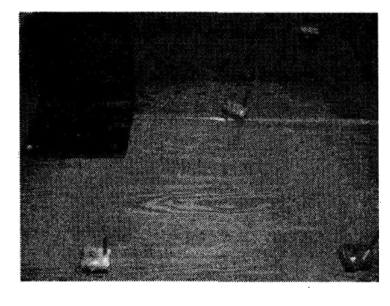


图 11.16　节点定位算法测试平台

当目标节点的 x 坐标为 3 时，x 坐标定位误差试验结果如图 11.17 所示，对于 $R=5$m 和 $R=10$m 各进行 10 次试验，每次试验测试 50 组数据并取平均值。从图中可以看出，增加锚节点的距离 R，可在一定程度上减小定位误差。

当目标节点的 y 坐标为 4 时，y 坐标定位误差试验结果如图 11.18 所示。

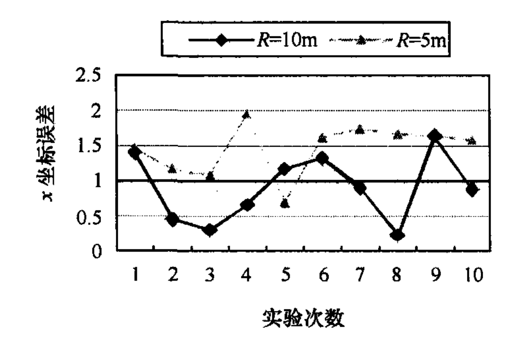


图 11.17　x 坐标定位误差曲线（单位：m）

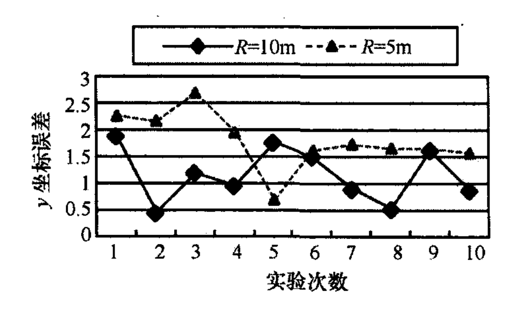


图 11.18　y 坐标定位误差曲线（单位：m）

11.4　节点定位过程中的安全问题

11.4.1　攻击样式

和其他过程一样，节点定位也存在安全问题。一方面，用于定位的信息必须经过认证，不得被恶意篡改；另一方面，在需要时能提供这些信息。

在介绍具体的安全定位算法前，先分析一下攻击模型以了解攻击者的能力。攻击者可以是内部攻击者也可以是外部攻击者：内部攻击者能访问节点密钥，并成为网络合法成员。基于密码和其他加密机制的认证对策无法阻止此类攻击；外部攻击者无法获取节点密钥信息、用于认证的密码等，只能物理捕获节点。

回放式攻击（Replay Attack）：回放式攻击是最简单且被广泛使用的攻击方法，特别是当攻击者能力有限时，即攻击者只能危害一个节点。这种攻击方式通过截获两个节点间传输的信息，并伪装成其中的发送节点向接收节点回放陈旧的定位信息。如图 11.19(a) 所示，节点 A 向节点 C 回放其接收到的节点 B 的信息。

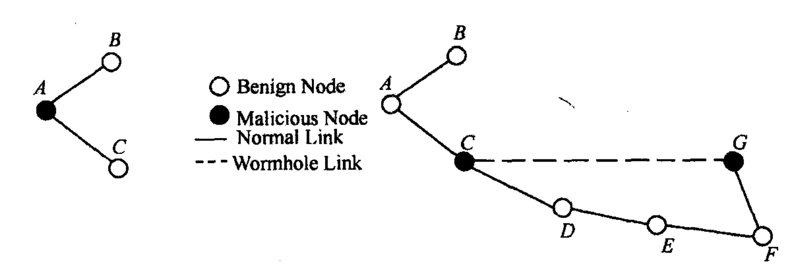


图 11.19　回放与虫洞攻击实例

(a)回放式攻击实例；(b)虫洞攻击实例。

女巫攻击(Sybil Attack)：对于女巫式攻击，攻击者能在网络中扮演多种角色，从而向接收节点发送多种位置参考信息，干扰定位信息的可靠性。

虫洞攻击(Wormhole Attack)：虫洞攻击是最为复杂的攻击方式，攻击者至少要干扰两个节点。在如图 11.19(b)所示的网络中，节点 C 和 G 为攻击者，A 向 B 和 C 发送位置参考消息时，由于 C 和 G 之间存在虫洞链路，G 能向邻节点 F 回放 A 的位置参考消息，导致节点 F 错误估计自己的位置。直观地，虫洞攻击对非基于距离的定位算法的危害高于基于距离的定位算法。

此外，还有移走锚节点、增加恶意距离、错误位置及距离的传播等攻击样式。

11.4.2　安全定位系统及算法

近年来，定位过程中的安全问题得到越来越多研究人员的重视，典型的安全定位系统及算法有 SeRLoc、Beacon Suite、鲁棒统计法、SPINE、ROPE、DRBTS 和 HiRLoc 等。

1. SeRLoc 算法

在文献[21]中，Lazos 和 Poovendran 提出一种非基于距离、分布式、资源有效的 SeRLoc 安全定位算法。该算法对虫洞、女巫等攻击具有鲁棒性。网络节点被分成两类：N 为装有欧米尼定向天线的节点，即目标节点；L 为装有定向天线的节点。定位过程中，锚节点向目标发送包含锚节点坐标、定向天线边缘线与坐标系的夹角的定位信息。节点 S 经过 4 步确定其位置：第一步，节点收集其周围锚节点的定位信息；第二步，根据定位信号确定近似搜索区域；第三步，采用多数选举机制，计算天线重叠区域；第四步，将重叠区域的重心作为目标节点的位置估计。

在布置节点前，向目标节点和锚节点预装共享对称密钥，未采用非对称密钥加密主要因为节点计算和存储资源有限。由于共享对称密钥无法确定信息源，这样攻击者就可攻击多个锚节点。为了阻止此类攻击，禁止节点访问共享密钥并向网络注入错误的位置信息，利用防冲突的哈希函数(Collision Resistant Hash Function)对定位信号进行认证。哈希序列产生过程如下：

$$H^0 = PW_i,\quad H^i = H(H^{i-1}),\quad i = 1,2,\cdots,n \tag{11.27}$$

2. Beacon Suite 算法

Liu，Ning 和 Du 在文献[22]中提出一系列用于检测恶意锚节点的技术，包括检测恶意定位信号、过滤回放的定位信号、恶意节点的识别和误检测的避免等，最终废除恶意攻击节点。在此安全定位机制中，锚节点既提供定位信号又检测其他锚节点的定位信号，锚

节点无需被动侦听定位信号,可通过发送请求的形式主动获取位置信息。

废除机制基于每个锚节点维护的告警和报告两种计数器,其中,告警计数器记录可疑锚节点;报告计数器记录该可疑节点报告并被基站接收的告警数。当某个锚节点行为异常时,向基站报告。

3. 抵抗攻击的位置估计法

Liu,Ning 和 Du 在文献[23]中提出两种基于距离鲁棒定位方法,能抵抗恶意攻击。第一种方法通过检测锚节点定位信号的一致性,并利用最小二乘估计,过滤恶意定位信号;第二种方法采用迭代精练的选举机制能抵抗恶意攻击。即使恶意攻击通过验证,这两种方法都能不受影响。

4. 鲁棒统计法

Li,Trappe 和 Zhang 等人在文献[24]中提出利用网络各个层次信息的冗余性应对恶意攻击,而非过滤攻击,并给出两类基于统计的安全定位。对于三角测量定位,采用自适应最小二乘和最小中值估计器,当遭受攻击时切换到最小二乘估计鲁棒模式;未遭受攻击时,采用最小二乘估计,计算复杂度低。对于基于 Finger Printing 的定位,传统的欧氏距离作为指标难以满足安全需求,作者利用基于中值的最近邻节点机制应对攻击。这两种方法的前提是良性观测数多于恶意观测。

5. SPINE 算法

SPINE(Secure Positioning In sensor NEtworks)是 Capkun 和 Hubaux 在文献[25]中提出的基于可验证的多边测量(Verifiable Multilateration),存在攻击时能保证安全计算及验证节点位置。SPINE 将每个节点的位置信息与至少 3 个节点关联,攻击者只能增加距离信息,通过纳秒级时钟,每个节点能和任意邻节点绑定距离。如果节点在 3 个参考节点形成的三角形区域内,则可基于 VM 技术计算节点位置。但 SPINE 也有缺点,为了执行 VM,需要大量参考节点,且属于集中式算法。

6. ROPE 算法

ROPE(RObust Position Estimation)是一种混合式安全定位算法[26],有两方面优点:无需任何集中式计算,即可决定节点位置;提供位置认证机制。为了衡量 ROPE 对攻击的抵抗性能,Lazos 提出了一种新颖的衡量指标——最大欺骗效果(Maximum Spoofing Impact)。仿真结果表明,ROPE 算法能在布置少量参考节点的情形下,达到较低的最大欺骗效果。与 SPINE 相比,ROPE 对于阻塞攻击的性能略差。

7. DRBTS 算法

DRBTS(Distributed Reputation-based Beacon Trust System)是一种分布式安全定位算法[27],是对 Beacon Suite 算法的扩展。在定位过程中可排除恶意节点提供的不正确位置信息,具体作方法为锚节点间相互检测定位信号,节点据此选择哪些锚节点可以信任。只有当锚节点的半数以上邻节点通过对锚节点检测后,该节点的定位信号才可靠。仿真结果表明,随着节点密度的增加,DRBTS 算法具有鲁棒性。由于 DRBTS 是分布式的,既在很大程度上可减轻基站的负担,又可有效减小恶意节点的破坏。

8. HiRLoc 算法

HiRLoc(High resolution Range-independent Localization)是一种与距离无关的定位算法[28],通过锚节点交叉覆盖区域的方式进行定位,每个定位信号采用全局对称密钥,可有

效抵制虫洞攻击、女巫攻击等。与 SeRLoc 不同的是，目标节点可收到同一个锚节点的多个定位信号，可提高定位精度。

参考文献

[1] Neal P, Joshua A N. Locating the nodes: Cooperative localization in wireless sensor networks[J]. IEEE Signal Processing Magazine, 2005, 22(4): 54-69.

[2] Girod L, Estrin D. Robust range estimation using acoustic and multimodal sensing[C]. In: IEEE International Conference on Intelligent Robots and Systems. 2001, Vol. 3:1112-1120.

[3] Girod L, Bychovskiy V, Elson J. Locating tiny sensors in time and space: A case study[C]. In: Proceedings of the 2002 IEEE International Conference on Computer Design. Freiburg, 2002: 214-219.

[4] Niculescu D, Nath B. Ad Hoc Positioning System(APS) Using AOA[C]. In: Proceeding of IEEE Conference on Computer and Communications Societies, 2003, vol. 3: 1734-1743.

[5] Lewis G, Deborah E. Robust Range Estimation using Acoustic and Multimodal Sensing[C]. In: Proceedings of IEEE International Conference on Intelligent Robots and System, 2001:1112-1120.

[6] Harter A, Hopper A, Steggles P, etc. The anatomy of a context-aware application[C]. In: Proceedings of mobile Computing and Networking. 1999:59-68.

[7] Savvides A, Han C-C, Srivastava MB. Dynamic fine-grained localization in ad-hoc networks of sensors[C]. In: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, 2001:166-179.

[8] Savvides A, Park H, Srivastava M B. The bits and flops of the N-hop multilateration primitive for node localization problems[C]. In: Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications. New York, USA: Association for Computing Machinery, 2002. 112-121.

[9] Capkun S, Hamdi M, Hubaux J P. GPS-Free positioning in mobile ad-hoc networks. Cluster Computing[J], 2002, 5(2):157-167.

[10] Iyengar R, Sikdar B. Scalable and distributed GPS free positioning for sensor networks[C]. In: Proceeding of IEEE International Conference on Communications. 2003, vol. 1: 338-342.

[11] Xiaoli Li, Hongchi Shi, Yi Shang. A map-growing localization algorithm for ad-hoc wireless sensor networks[C]. In: Proceedings of the Tenth International Conference on Parallel and Distributed Systems. Los Alamitos, USA: IEEE Computer Society, 2004:395-402.

[12] Niculescu D, Nath B. Localized Positioning in Ad Hoc Networks[J]. Ad Hoc Networks, 2003, 1(2): 247-259.

[13] Benbadis F, Friedman T. GPS-Free-Free Positioning System for Wireless Sensor Networks[C]. In: IEEE International Conference on Wireless and Optical Communications Networks. 2005: 541-545.

[14] Yi Shang, Wheeler R, Ying Zhang. Localization from mere connectivity[C]. In: Proceeding of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing. 2003: 201-212.

[15] Bulusu N, Heidemann J, Estrin D. GPS-less Low Cost Outdoor Localization for Very Small Devices[J]. IEEE Personal Communications Magazine, 7(5): 28-34.

[16] He T. Range-free Localization Schemes for Large Scale Sensor Networks[A]. Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (Mobicom2003)[C]. San Diego, CA, USA, September, 2003:14-19.

[17] Niculescu D, Nath B. DV Based Positioning in Ad Hoc Networks[J]. Telecommunication Systems, 2003, 22(1):267-280.

[18] Radhika Nagpal, Howard Shrobe, Jonathan Bachrach. Organizing a global coordinate system from local information on an Ad hoc sensor network[A]. Proceedings of the 2nd International Workshop on Information Processing in Sensor Networks (IPSN'03)[C]. Palo Alto, CA, USA, 2003.4: 333-348.

[19] Doherty L. Algorithms for position and data recovery in wireless sensor networks[D]. University of California Berkeley, 2000,6.

[20] Mark P J. Localization from mere connectivity[A]. Proceedings of the Mobile ad hoc networking and computing[C]. MOBIHOC 2003, Annapolis, Maryland, USA.

[21] Lazos L, Poovendran R. SeRLoc: Secure range independent localization for wireless sensor networks[C]. In ACM workshop on Wireless security (ACM WiSe '04), Philadelphia, PA, October 1 2004.

[22] Liu D, Ning P, Du W. Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks [C]. 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), pp. 609 - 619, 2005.

[23] Liu D, Ning P, Du W. Attack-Resistant Location Estimation in Sensor Networks[C]. In Proceedings of The Fourth International Conference on Information Processing in Sensor Networks (IPSN '05), pp. 99 - 106, April 2005.

[24] Li Z, Trappe W, Zhang Y, etc. Robust statistical methods for securing wireless localization in sensor networks[C]. In Proceedings of IPSN '05, 2005.

[25] Capkun S, Hubaux J - P. Secure positioning of wireless devices with application to sensor networks[C]. In Proceedings of IEEE INFOCOM '05, 2005.

[26] Lazos L, Poovendran R, Capkun S. ROPE: Robust Position Estimation in Wireless Sensor Networks[C]. In the Proceedings of the 4th international symposium on Information processing in sensor networks, IPSN '05, 2005.

[27] Srinivasan A, Teitelbaum J, Wu J. DRBTS: Distributed Reputation-based Beacon Trust System[C]. 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), pp. 277 - 283, 2006.

[28] Lazos L, Poovendran R. HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Communications, VOL. 24, NO. 2, February 2006.

第 12 章　无线传感器网络接入技术

实际应用中,无线传感器网络所处的监测环境往往十分恶劣,用户无法在现场收集数据。对于某些用于监测环境监测的网络,人在监测现场还会干扰被测对象,影响测试结果的可靠性。类似的需求与特点决定了只有将无线传感器网络与现有信息网络互联,让用户在远端实时共享传感器网络的监测结果,实现物理世界与逻辑世界的互联,才能充分发挥无线传感器网络的作用。

12.1　接入技术概述

无线传感器网络通过基站与外部信息网络相连,研究人员可以通过外部信息网络远程控制无线传感器网络的工作。如果监控的地点非常偏远,一般选择卫星链路用作基站和因特网的连接。在因特网上通常还有一个中心服务器负责控制和协调传感器网络的工作并保存传感器网络发送的数据。由于基站通常处于无人值守的状态,需要基站以及基站到中心服务器的链接具有高可靠性。基站需要对可能的系统异常及时进行处理。如果系统崩溃,基站需要及时地重新启动系统并主动连接中心服务器,以使远程控制人员能够恢复对传感器的远程控制。

远程任务控制最主要的方面是重新安排无线传感器网络的监控任务。研究人员往往会在监控一段时间后调整传感器网络的监控任务,这样的变化需要通过远程控制的方法传达到整个传感器网络。研究人员向基站发出任务更改指令,通常情况下基站会周期性地广播一个网络保持消息,并将任务更改指令包含在网络保持消息中。更为复杂的情况是需要更新节点上运行的程序。基站节点将新程序的二进制映像发送到每个节点,节点启动自我更新程序将新程序写人。但更新程序消耗能量很多,不能频繁进行。

远程任务控制还需要监控传感器节点的工作状态以及健康情况,并据此调整节点的工作任务。节点的健康状况包括剩余能量、传感器部件、通信部件的工作情况等。通过监控传感器节点的工作状态,可以及时调整传感器节点的工作周期,重新分配任务,从而避免节点过早失效,延长整个网络的生命期。目前主要通过节点的工作电压判断节点的剩余能量信息。节点周期性地采样自己的工作电压,依据 3.3V 的标准电压归一化处理,并将结果通知网关节点。如果节点的电压值过低,该节点读取的传感数据的可靠性也大大降低,因此需要延长电压过低节点的休眠时间并减少采样频率。

为实现无线传感网络接入外部信息网,保证接入安全性、系统可用性和可扩展性,目前国内外研究内容包括以下几方面[1]:

(1)复合型无线传感网络接入互联网模型。分析基于代理、DTN 网络和网状网结构的接入方式优缺点,研究一种复合型接入模型。

(2)网关数目和无线传感网络规模关系模型。建立数学模型,研究在具体性能要求下,网关节点数目和无线传感网络规模之间的关系。

(3)多网关动态部署、移动策略、负载均衡、容错机制。研究网关位置的动态部署理论;研究移动网关的移动策略,提高接入性能。研究数据请求的分发策略和迁移策略,实现网关负载均衡;研究多网关容错机制,保证部分网关失效时接入的可用性。

(4)轻量级网关访问控制、数据验证和高效抗 DoS 攻击机制。研究网关的访问控制机制,保证数据机密性;研究网关的数据验证机制,保证数据真实性。研究检测和抵抗 DoS 攻击的机制,应对来自互联网和无线传感网络内部的双重 DoS 攻击。特别地,由于网关资源仍然受限,所以需要研究轻量级的安全机制。

(5)适用于无线网状传感网络的通信协议。研究节点到无线路由器间的短距离数据传输;研究节点和路由器之间的信道分配问题;研究节点到路由器的路由建立机制;研究路由层和链路层的跨层优化问题。

(6)基于无线网状网的传感节点的移动性支持。研究维护动态的节点拓扑及路由器切换问题;研究轻量级的分布式节点移动性管理机制;研究无线传感网络多网关和无线网状网理论和方法,根据实际应用解决大规模传感网络接入互联网的关键理论问题,提出面向新一代网络技术的无线传感网络接入互联网解决方法。

12.2　接入方式研究现状

无线传感器网络的接入方式是指,采用何种结构设计 Sink 节点,利用何种通信技术与终端用户进行信息交互,以及采用何种形式提交监测信息,以实现无线物理世界和虚拟的世界的无缝互联。根据此定义,Sink 节点接入方式是指其采用何种手段接入外部总线或网络,将信息传送至终端用户。

12.2.1　代理接入方式

代理接入方式是指 Sink 节点通过某种通信方式接入基站,以基站作为代理接入到终端用户所在的互联网,如图 12.1 所示。传器节点将采集到的数据传送给 Sink 节点,然后经由某种总线方式或专用网络传送给基站,基站是一台可以和互联网相连的计算机,它将数据通过互联网发送到数据处理中心,同时它还具有一个本地数据库以缓存数据。终端用户可以通过授权接口连入网络访问数据中心,或者向基站发出命令。

至于 Sink 节点采用何种方式接入到基站,以实现传感器数据流的传送,国内外研究者面向各种具体应用,采用了不同的方式。如著名的大鸭岛生态环境监测系统采用 Stargate 信号接收机及卫星通信传输系统接入基站,Intel 公司为美国俄勒冈州设计的葡萄园环境监测系统[2]通过 CAN 总线实现接入;我国宁波中科集成电路设计中心设计的无线传感器网络实验平台采用的是串口和 USB 口接入方式;为了适应工程需求,招宝山大桥斜拉索振动监控系统使用 GPRS 通信方式实现 Sink 节点接入基站。

这种接入方式适用于传感器网络工作在安全,且距离用户较近的区域。其优点在于利用功能强大的 PC 作为网关执行网络接入任务,减少 Sink 的软硬件复杂度,进而减小 Sink 的能耗;此外,这种结构还可将 Sink 收集的数据实时传输到网关,在网关存储、处理和决策。

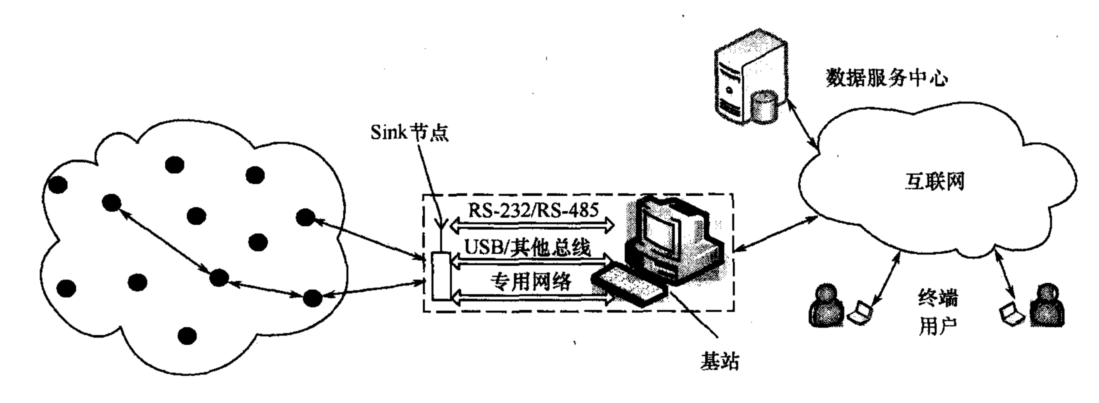


图12.1 基于代理的Sink节点实现方式

代理方式的缺点也很明显，利用PC作为网关的代价和体积均较大，不便于布置，在恶劣的环境中无法正常工作，尤其在军事应用中不利于网络节点隐蔽，容易被敌方发现。

12.2.2 直接接入方式

直接接入方式是指Sink节点直接接入终端用户所在网络，这种方式是当前研究重点和发展趋势。文献[3]提出了一种基于PDA的移动嵌入式Sink节点，该节点利用IEEE802.11g无线通信协议接入终端用户所在的无线局域网。文献[4]设计了基于CDMA模块的Sink节点实现方案，通过它的协议转换功能，连接无线传感器网络和CDMA网络。文献[5]提出了Sink节点通过接入中国移动GSM网络，将传感器采集数据传送到处于该网络上的终端用户。

在图12.2所示的接入方式中，Sink既可通过无线通信模块和监测区域内的节点无线通信，又可利用低功耗、小体积的嵌入式Web服务器接入以太网，实现天线传感器网络内部和以太网的隔离。这样，在传感器网络内部可以采用更加适合无线传感器网络特点的MAC协议、路由协议和拓扑控制等协议，实现网络的能量有效性、扩展性和简单性等目标。另外，在嵌入式Web服务器上可运行轻量级TCP/IP协议，并通过加入安全认证机制，能提高传感器网络与以太网互联的可靠性。

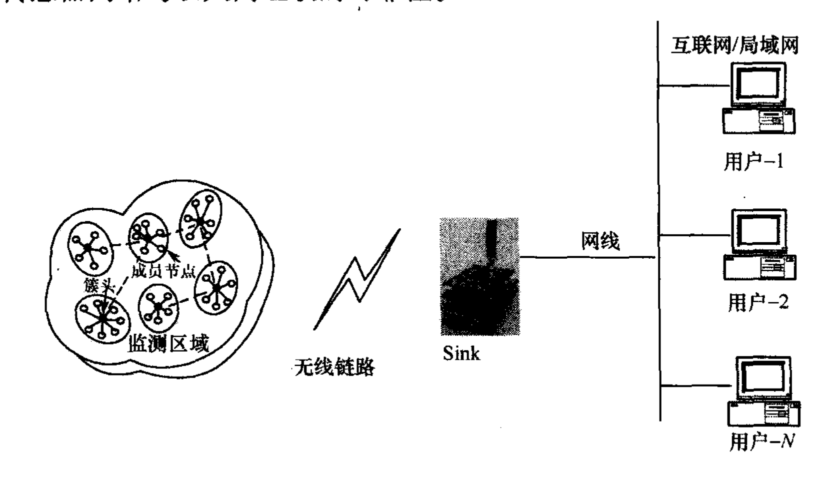


图12.2 直接接入方式

12.3　无线传感器网络接入因特网

目前,国内外对无线传感器网络与因特网互联的研究尚处于初级阶段。归纳已有的研究成果,无线传感器网络与因特网互联的主要内容是如何利用网关或IP节点,屏蔽下层无线传感器网络,向远端的因特网提供实时服务,并且实现互操作[6]。将无线传感器网络接入互联网将面临一些挑战,其原因在于无线传感器网络与因特网相比有显著的区别。

1. 数据流模式

无线传感器网络的基本用途是将每个传感器节点视为一个单独的数据采集装置,进而可以将无线传感器网络视为分布式数据库,而用户节点相当于数据库前台。因此,一对多和多对一的数据流是无线传感器网络通信中的主要模式,而传统IP网络以一对一的数据流为主。

2. 能源限制

通常情况下,传感器节点以电池供电,并且基本不具备再次充电的能力。在这种情况下,网络的主要性能指标是网络运转的能源消耗。由于通信的能耗高于计算的能耗,这样就使得无线传感器网络的协议设计必须遵循最小通信量原则,有时甚至需要牺牲其他网络性能,如延迟和误码率等。这一点与传统IP网络截然不同。

另外,互联网是围绕着以地址为中心的思想设计的,网上流动的数据通常对应着特定源和目的地址,而以地址为中心的思想并不适于无线传感器网络。

12.3.1　网络互联结构

无论是采用同构还是异构的网络结构,作为流量瓶颈的无线传感器网络的因特网接入节点都是非常重要的。一个值得注意的问题是,对接入点位置、状态可能发生变化的无线传感器网络来说,在接入节点中的汇聚点移动或者失效的情况下,还需要保持与因特网的通信。为实现上述目标可能需要设计一种新的方案,使无线传感器网络与因特网的接口能够比较稳定地工作。它应该具备以下条件:

(1)移动的接入节点在改变了位置或者失效之后,无线传感器网络还能够保持与因特网的正常通信,或者保持实时数据的完整性。

(2)与移动节点通信的因特网上的主机不需要改变其协议。

(3)移动节点接入的因特网链路可能是无线链路,因此带宽较窄、误码率较高,移动节点发送的管理报文应该尽可能少,以减少开销。

简单易行的解决办法如下:

(1)赋予无线传感器网络多个连接因特网的接口,这种方法使得网络管理成本提高,并且加大了通信能耗,会产生大量的冗余信息。

(2)使用能力更高的节点、更先进的设备以确保链路畅通,这样会导致无线传感器网络优势的丧失。

(3)将待传输的数据信息存储在本地节点上,事后手工恢复通信。

很明显,这几种方式都不适合大规模的无线传感器网络。移动代理技术也许可以成

为比较理想的解决手段之一。移动代理是一个代替人或其他程序执行某种任务的程序，在复杂的网络系统中能自主地从一台主机移动到另一台主机。在移动时，该程序可以根据要求挂起其运行，然后转移到网络的其他节点重新开始或继续其执行，最后返回结果和消息。移动代理的自主性使得移动代理能在没有人或其他代理直接干预和指导的情况下持续运行，并能控制其内部状态和动作。针对前文的要求，可以考虑在通信移动代理中封装与因特网通信功能模块。当代理所在节点将要移出通信范围或者耗尽能量，导致与因特网断开链接，移动代理可以携带有用信息，选择转移到附近的合适节点，使之成为接入节点。

另外，在与因特网的交互过程中，通常由于移动节点的物理位置不停地改变，要不断地维护和重新配置当前的数据链接，一旦这种连通性不能及时地维持，就需要额外地处理脱线阶段的交互数据。在这类应用中，采用移动代理技术非常有利。远端用户可以在所发出的数据移动代理中事先封装所需的长期交互过程中的所有信息，由该代理程序携带用户的查询请求，发送至无线传感器网络并在其上运行，与网关或接入节点进行所需的交互。这期间无线传感器网络与因特网的链接甚至可以中断而不会影响移动代理程序的工作。当代理程序工作结束后，如果链接恢复，代理即可将交互结果返还给远端用户。

12.3.2　基于嵌入式 Web 服务器的互联结构

在图 12.3 所示的嵌入式 Web 服务器体系结构[7]中，外设接口用于数据采集和控制输出接口。数据处理单元的一个任务是对采集到的信号进行处理和相应地补偿。数据传输单元的基本功能是实时操作系统统一协调和管理下，通过 TCP/IP 通信协议栈和网络接口实现数据的双向传输，利用嵌入式 Web 服务器内的芯片 Web 服务器功能，使用户能够通过客户端标准的浏览器和传感器网络系统进行交互的网络会话，为用户提供一种方便的数据采集和控制手段，通过设定相关系统参数，实现数据采集/控制，并可以即插即用。

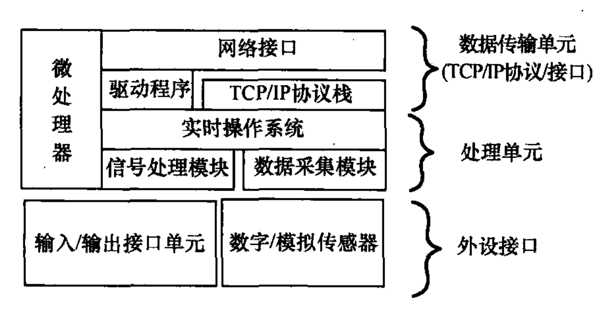


图 12.3　系统体系结构图

图 12.4 是基于分层无线传感器网络构建的一种基于嵌入式 Web 服务器网络的互联结构[8]，这种接入方式结构清晰。这种无线传感器网络结构克服了分级结构扩展性差的缺点，可实现智能路由，降低延时并增强网络连接性。虽然射频通信的时变特性会引起节点间通信的时断时续，但无线传感器网络的整体拓扑结构是相对稳定的，因此降低了接入互联网的难度。

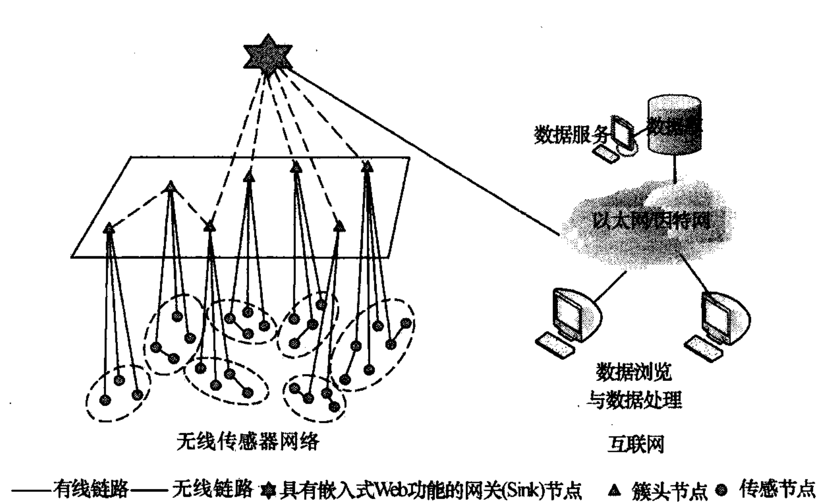


图 12.4　基于分层的无线传感器网络与因特网的互联

12.4　Sink 的多接入模式

为了使用户利用现有网络设备接入原型系统，尽可能方便地使用监测系统的相关信息，Sink 节点可利用多种模式接入原型系统，包括 RS－232C 直接接入、互联网接入、有线远程拨号接入和无线远程拨号接入。

1. 本地直接接入

对于短距离应用，可通过 Sink 节点的 RS-232C 接口直接与 PC 机或使用数据的现场设备互联，系统结构如图 12.5 所示。

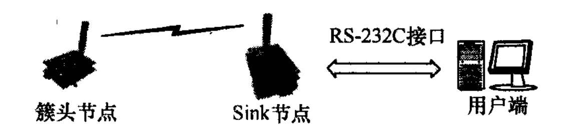


图 12.5　本地直接接入的系统结构

2. 互联网接入

通过 Sink 节点的 RJ45 接口与交换机连接，本地或异地用户通过 IP 地址访问 Sink 节点获取数据，系统结构如图 12.6 所示。

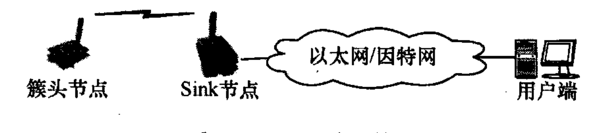


图 12.6　互联网接入

3. 有线远程拨号接入

有线远程拨号是个人 PC 机接入互联网的一种方式。Sink 节点通过 RS－232C 接口与标准 56Kb/s 调制解调器连接，将数字信号变换为模拟信号向公共交换电话网(Public Switched Telephone Network，PSTN)上发送；接收方通过 56Kb/s 调制解调器将模拟信号变

换为数字信号提交给远程用户通信终端，系统结构如图 12.7 所示。



图 12.7　有线远程拨号接入

这种方式同一时间只允许一个用户访问 Sink 节点，开发工作主要完成 RS－232C 串口初始化和 56Kb/s 调制解调器的初始化设置。调制解调器初始化工作主要是通过 AT 命令对本地调制解调器进行设置，对于平台的 DTR、RTS 等同步信号则忽略，初始化关键代码为：

```
void Modem Init()
  {
      put_str("ATE0Q0V0W0S0 =1&C1&D0&R1&K0&S0&Y0&W0?);
  }
```

实验证明，在 Sink 节点传送数据量不大的情况下，这样做不会造成通信质量的下降，且只要在有电话线的地方用户就可以远程访问 Sink 节点。

4. 无线远程拨号接入

GSM 模块是传统调制解调器与 GSM 无线移动通信系统相结合的一种数据终端设备，亦称无线调制解调器[9]，凡使用调制解调器的地方大多可用 GSM 模块代替。TC35IT 是基于 GSM 模块 TC35 的数据终端设备，支持语音、数据、短消息和传真服务，向用户提供标准的 AT 命令接口。基于 TC35IT 的无线远程拨号接入方式如图 12.8 所示。

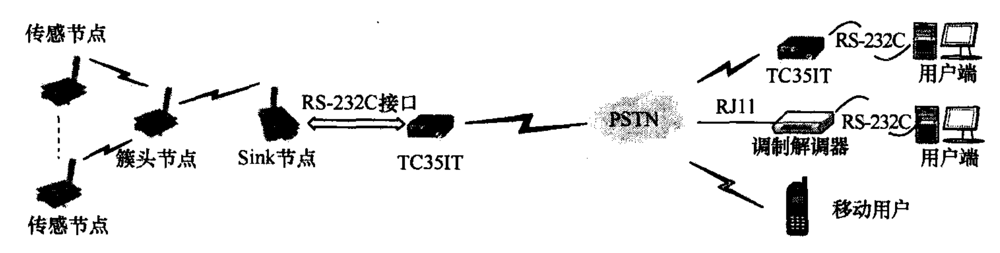


图 12.8　基于 TC35IT 的无线远程拨号接入

基于 TC35IT 可开发短消息和 IE 浏览器页面两种测控方式[10]。

1）短消息方式

在 GSM 中，唯一不需建立端到端通道的业务就是短消息业务。也就是说，它不用拨号建立连接，直接把要发的信息加上目的地址发送到短消息服务中心，由短消息服务中心再发送给最终的信宿。因此，短消息监控的优点在于其无需建立连接，服务费用低，可以实现用户随时随地从 Sink 节点获取数据。尤其在无法建立无线通信网络的条件下，可以利用 GSM 短消息接口进行数据和控制指令传输，这样可以大大节约成本。

2）IE 浏览器页面测控

这种方式使用无线调制解调器。客户端需要建立拨号网络，通过拨叫服务器端 SMS 卡数据号和服务器建立连接，连接后使用 IE 访问 Sink 节点获取数据。

5. 与 CDMA 网络互联

理论上说，Sink 可以采用任意网络技术接入外部网络。但在实际应用中选择 Sink 的

接入方式时，首先应该考虑的是无线传感器网络的应用环境所能提供的、可能的网络接入方式；其次，与现有网络相比，无线传感器网络是一种以数据为中心的网络，Sink 节点的上行数据量大而下行数据量小。

因而，在考虑 Sink 与外部网络的连接方式时，上行数据率是一个关键指标。Sink 节点的成本及集成难度也是一个关键因素。综合考虑以上因素，中国电信的 CDMA 1X 网络在网络覆盖、数据传输速率、网络的稳定性和节点性价比上都有优势，因而，决定选用 CDMA 技术作为 Sink 与监控中心的空中接口。

如上所述，采用 CDMA 1X 网络作为 Sink 与监控中心的接入网络，则 Sink 节点作为两个异构网络的接口，应该包含这两种网络的协议栈，并完成协议之间的转换。实际上，Sink 的作用就在于通过协议的转换来连接两个异构的网络。要弄明白 Sink 如何处理网络节点传输来的数据，首先就必须搞清楚网络节点处理传感器部件采集到的数据的过程。

网络节点获得传感数据后，应用其操作系统上的应用软件对数据进行简单的处理，然后以一定的格式存储到其存储器上。在需要将数据传输到 Sink 时，网络节点按照无线传感器网络的协议规范，将数据进行封装，然后通过空中接口经过路由协议将数据传送到 Sink。传感数据在通过物理介质进入 Sink 后，先用无线传感器网络的协议栈解封装，得到原始数据之后，Sink 可应用其操作系统上的应用软件根据具体需求对原始数据进行处理，如进行数据聚集、去除冗余数据、减轻 Sink 对外传送的负担。处理后的数据经由 TCP/IP 模块打包后通过串口与 CDMA 通信模块相连。最后，Sink 中的 CDMA 模块将数据通过空中接口 Um 传送到 CDMA 骨干网上。

与 CDMS 互联的 Sink 的协议栈模型如图 12.9 所示。

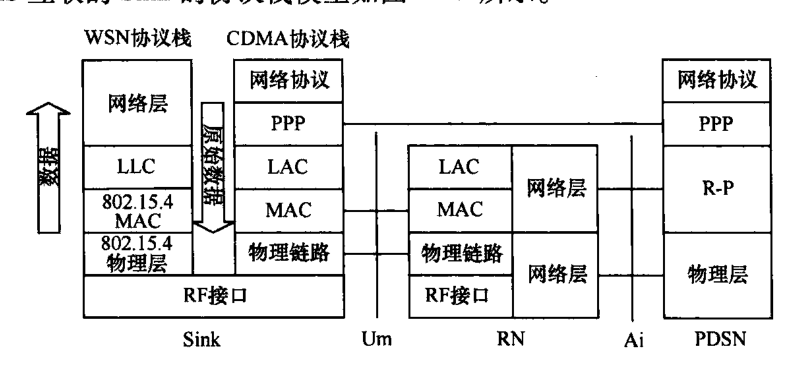


图 12.9　Sink 协议栈模型

图 12.9 中，Sink 包括无线传感器网络和 CDMA 的协议栈，其中，无线传感器网络协议栈采用了 IEEE802.15.4 定义的物理层和 MAC 层。RN 是指 CDMA 无线网络，它包括基站控制器、基站收发信系统和分组控制功能。PDSN 是指分组数据服务节点，从互联网的角度来看，它是一个路由器，并根据移动网的特性进行了增强。Um 为 Sink 与 RN 的空中接口，它由物理链路、MAC、链路访问控制(Link Access Control，LAC)组成。RN 和 PSDN 间的接口，即 R－P 接口，在 CDMA2000 系统中被看作 A 接口的一部分，叫做 A10 和 A11。PPP 协议是 IP 协议集中的一个重要组成部分，它完成拨号功能，建立 Sink 与 CDMA 核心网的点对点链路。

利用 Sink 实现无线传感器网络与 CDMA 网路的互联时，Sink 主要由控制模块、无线

传感器网络协议处理模块、TCP/IP 协议处理模块、PPP 协议处理、无线传感器网络无线模块和 CDMA 通信模块组成，如图 12.10 所示。

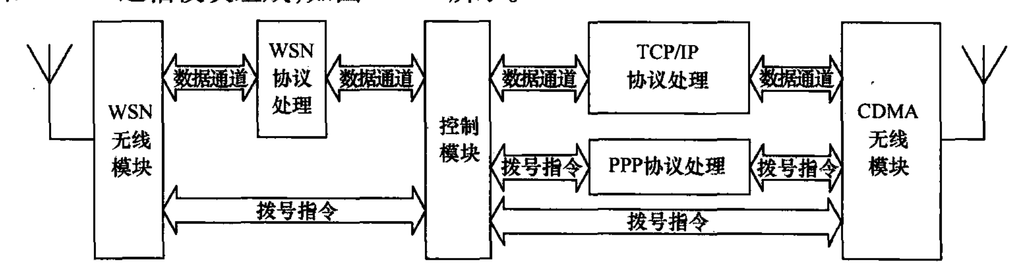


图 12.10　与 CDMA 互联的 Sink 结构

6. 控制模块

控制模块的主要功能是通过无线传感器网络通信模块接收传感器节点的数据，对无线传感器网络通信模块进行配置管理；通过 AT 指令初始化 CDMA 通信模块，利用 PPP 协议将 Sink 连接到 CDMA 网上，获得网络运营商动态分配给 CDMA 模块的 IP 地址，并与监控中心终端或服务器之间建立连接。

控制模块可以采用 Atmel 公司的 AT91RM9200 微处理器，它是基于 ARM920T 指令集的 ARM 处理器。该处理器具有丰富的外设以及接口，这使得它在低成本、低功耗的条件下能完成一些功能丰富的应用。AT91RM9200 处理器集成了许多外设接口，包括 USB2.0 接口和以太网接口。此外，该处理器还提供了多个符合工业标准的通信接口，包括音频、电信、闪存卡、红外、智能卡接口等。

7. CDMA 通信模块

CDMA 通信模块包括 CDMA 的 MAC 层协议栈软件、CDMA 基带、CDMA800/1900 的 RF 器件，其主要功能是把经过 TCP/IP 协议栈处理过的数据包和从基站接收的 CDMA 分组数据进行相应的协议处理后再转发。

CDMA 模块可采用 Wavecom 公司的 Q2338/Q2358。该模块使用高通 MSM6050 芯片组，利用了高通 gps One 技术地点定位功能。体积小巧，能轻松兼容各种手机和个人数字助理设备。

8. WSN 无线模块

无线传感器网络的无线模块包括无线传感器网络基带和无线传感器网络 868/915/2400 RF 部件，该模块的主要功能收发并处理无线传感器网络射频信号，并按照 IEEE802.15.4 协议要求完成无线传感器网络基带处理。IEEE802.15.4 协议在 3 个频段上共定义了 27 个物理信道，868MHz 频带上一个速率为 20Kb/s 的信道、902MHz～928MHz 频带上 10 个速率为 40Kb/s 的信道以及 2.4GHz 上 16 个速率为 250Kb/s 的信道。由于 2.4GHz 频带有 16 个物理信道，且数据速率可以达到 250Kb/s，应用前景更为广阔，因此，大多数芯片厂商都针对此频段开发了符合 802.15.4 协议的低功耗射频芯片。

Freecale 公司发布的 MC1319x 和 Chipcon 公司发布的 CC2420，是比较典型的产品。它们都采用 DSSS 扩频，O-QPSK 调制，有 16 个速率为 250Kb/s 的物理信道。CC2420 还支持部分 IEEE802.15.4MAC/PHY 功能，包括自动前导码生成、同步字插入与检测、16bit CRC 校验、MAC 层安全加密。

12.5　Sink 节点接入以太网通信传输协议研究

对于智能监测的应用而言,将无线传感器网络以某种方式集成到现有的 IP 网络是非常必要的。这使得远程用户能够获取实时环境下的数据。本章采用同构网络的结构使无线传感器网络接入以太网。同构网络是利用应用层 Sink 节点作为接口,屏蔽下层无线传感器网络,向远端的因特网用户提供实时的信息服务,并实现互操作。对于文本研究的中小型结构的无线传感器网络,Sink 节点可作为嵌入式 Web 服务器,传感器节点的数据经过传输被存储到 Sink 节点上,并以 Web 页的形式提供给用户。

12.5.1　嵌入式 TCP/IP 协议栈 μLwIP 的设计[11]

TCP/IP 协议栈本身是一种层式结构,所以在协议栈的设计上采用模块化思想,逐层实现,然后通过对各层接口函数的调用实现完整的协议栈。

12.5.1.1　TCP/IP 体系结构

嵌入式系统发展的方向是"软硬件相结合",即针对于特定的应用,软硬件是唇齿相依。任何软件的冗余都会对系统的资源及性能造成不必要的浪费和损害。TCP/IP 协议栈功能强大,包括众多协议,是一个通用型的通信传输协议套件,其功能覆盖了几乎全部互联网所提供的服务。而嵌入式系统往往只针对某个特定应用,使用完整的 TCP/IP 套件和机制,既浪费资源,又降低性能和效率、增加了功耗。

因此,根据无线传感器网络特点和智能监测的特定功能需求对 TCP/IP 协议体系进行合理的精简和优化,实现适合于 Sink 节点嵌入式 TCP/IP 协议栈"μLwIP"。TCP/IP 的 5 层协议参考模型如图 12.11 的左图所示,右图为本章研究的协议结构模型。

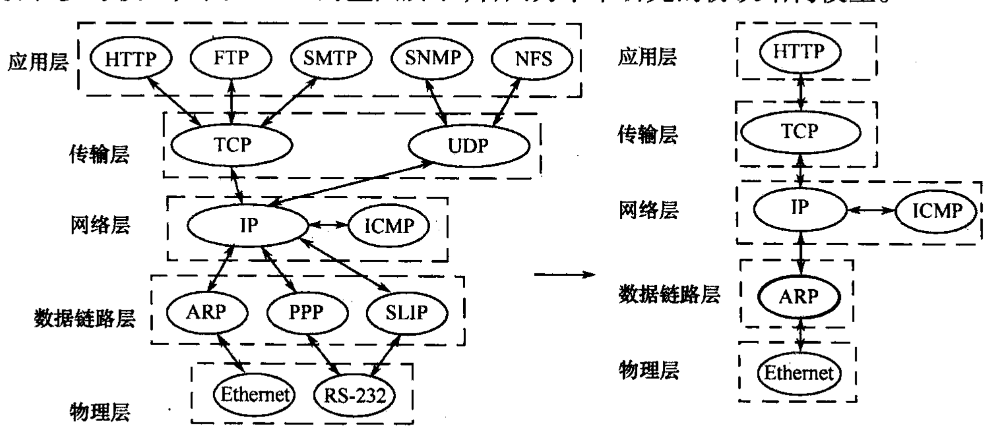


图 12.11　TCP/IP 协议体系模型

12.5.1.2　协议定制

嵌入式以太网技术作为 TCP/IP 协议的一种嵌入式应用,其功能是特定的。嵌入式 TCP/IP 协议栈 μLwIP 不要求实现所有的协议,其组成应该是 TCP/IP 的一个子集[12]。本文主要研究 TCP/IP 协议的 Sink 节点的实现和基于节点系统资源与能耗的保证正常网络通信与数据传输的协议精简模式,对协议组件进行精简、定制,降低嵌入式以太网技术的

实现难度，提出了精简 TCP/IP 协议栈 μLwIP。

在 μLwIP 中，传输层协议优化精简 TCP 协议；网络层协议优化精简 IP 协议和因特网控制消息协议 ICMP；数据链路层协议优化精简 ARP 协议；IP 协议是网络层的核心协议，而 ICMP 协议诊断网络连通情况的，本文基于简单的测试需求设定其实现类型和代码都为 0。在 μLwIP 之上，应用层协议优化精简 HTTP 协议。

基于嵌入式 TCP/IP 通信传输协议栈 μLwIP，本节建立了两种以太网通信机制。

1. μLwIP + applet + CGI + http

该方法利用在网页中嵌入 Java Applet 程序，实现数据的定时刷新。客户端和服务器通过 HTTP 连接进行请求的发送与响应，嵌有 Applet 程序的 HTML 页面文件，作为主页存放在服务器的存储器中，客户端通过 URL 对嵌入式 Web Server 中的资源进行定位，第一次访问 Web Server 时，Applet 被下载到客户端，并被本地的 Java VM 解释，进而触发 CGI 采集程序。由此，客户无需动态刷新整个 HTML 页面，而是在 Java Applet 定时启动 CGI 采集程序时，实现网页的动态刷新。

2. μLwIP + Socket

该方法利用 Socket 进行服务器和客户端的连接，Sink 节点系统工作时，服务器端 Socket 处于监听状态，客户端 Socket 只需根据服务器 Socket 的 IP 地址和端口号便可建立 TCP/IP 连接。连接建立后，客户端定时读取 Socket 中的信息，便可实现基于 Socket 方式的网页动态刷新。这种方式提高了连接效率和数据传输的效率，不需要浏览器，但需要在客户端安装应用程序。

12.5.2　μLwIP 层次协议设计

12.5.2.1　ARP 协议的精简与优化设计

嵌入式 Sink 节点要想接入以太网，就必须实现 ARP 协议。实现该协议可采用通用的 NIC 芯片，但以太网主机通信使用的是 48 位以太网地址，而 TCP/IP 协议使用的是 32 位 IP 地址。要想 TCP/IP 协议栈运行在以太网之上，必须进行地址解析。对应的协议是 ARP 和 RARP。ARP 负责将 IP 地址解析为以太网地址，对于 Sink 节点而言，本文将其设计成为嵌入式 Web 服务器，IP 地址存储在 Sink 节点内，不需要从其他服务器得到本机 IP 地址，因此 RARP 不需要。

1. ARP 协议的精简

ARP 协议包括 ARP 请求帧和 ARP 响应帧。ARP 请求帧用于系统主动向其他主机发送请求，目的是获得该主机的物理地址；ARP 应答帧是在收到其他主机发来的 ARP 请求帧后，应答本机物理地址。ARP 帧及相应的以太网帧格式如图 12.12 所示。

ARP 帧被封装在以太网帧的数据域中传输。TCP/IP 将它设计成一种能适应各种物理网络地址和协议地址的格式。在以太网接入方式中，无论是 ARP 请求还是应答，以下域都是固定不变的："类型"—0806（ARP 帧），"硬件类型"—0001（值"1"代表以太网），"协议类型"—0800（"0X0800"代表 IP 协议），"硬件地址长度"—06（以太网物理地址长度），"协议地址长度"—04（IP 地址长度），这些域值可以提前存储在一个固定的结构体里。由于本文只需要实现 ARP 协议，因此"操作"域只保留："1"为 ARP 请求，"2"为 ARP 响应。

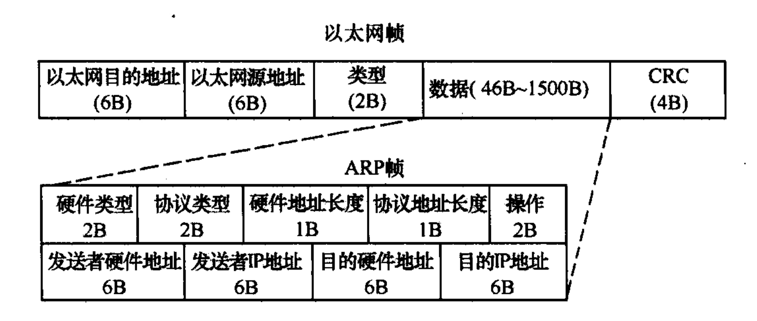


图 12.12　ARP 帧及其相应以太网帧格式

2. ARP 协议的实现

针对以太网广播特性,ARP 协议实现地址映射采用动态联编方法进行地址解析。ARP 响应过程如图 12.13 所示。当 Web 服务器发送数据到客户端时,如果客户端在本地局域网内,则目的 IP 即为客户端 IP 地址,如果不在局域网内,则交给默认网关转发,在 ARP 地址映射表中查找目的 IP 地址对应的物理地址,封装以太网帧并发送。若在 ARP 地址映射表中找不到客户端 IP 地址的记录,就发送一个 ARP 请求。ARP 请求协议的实现很简单,只是按数据帧格式封装请求帧即可。

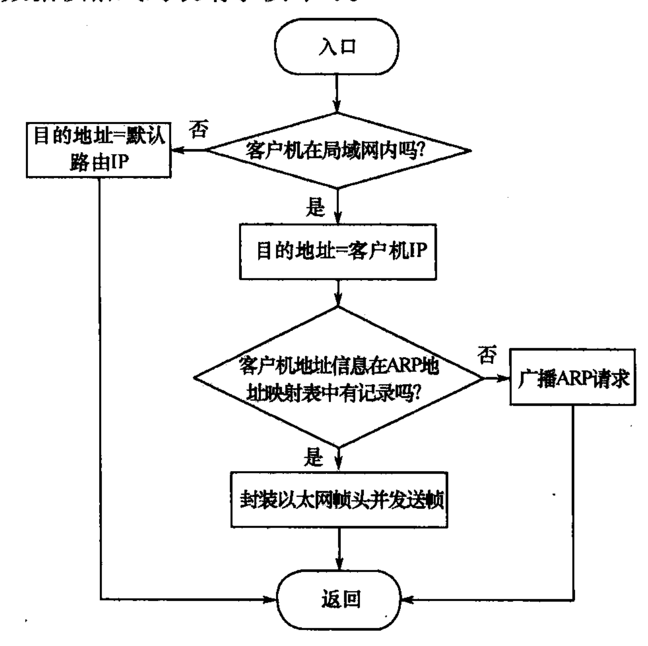


图 12.13　ARP 响应流程

建立一个大的 ARP 地址映射表可以减少 ARP 请求的次数,但是同时增大了 Sink 节点系统的开销。因此,本文根据 LPC2210 的资源建立相应大小的地址映射表,同时,每隔一定时间要更新映射表。在有新的连接时,给地址映射数组赋新数值即可更新 ARP 地址映射表。对于嵌入式以太网而言,客户端是随机的,而且 Web 服务器很少主动请求客户端的物理地址,所以可以建立一个容量为 1 的 ARP 地址映射表,即只保存当前连接地址映射[13],可大大减小内存的开销,降低节点系统功耗。μLwIP 协议栈调用 ARP 发送数据帧流程如图 12.14 所示。

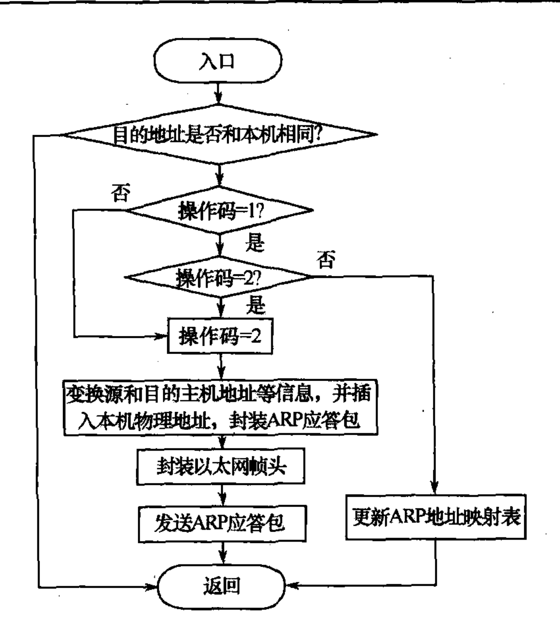


图 12.14 ARP 发送数据帧的流程

12.5.2.2 IP 协议的精简与优化设计

1. IP 协议的精简与优化

1)删除 IP 寻径、分片和重组

嵌入式 Sink 节点作为一个供用户访问的网络节点,仅实现主机功能即可,无需为网络转发数据帧,并且默认一个网关为初始网关。这样,在 IP 层实现的寻径表仅由两项构成,即当前连接的客户端 IP 地址信息和默认网关地址信息。

由于经 Sink 节点传输的数据量不大,IP 分片的情况很少,将 IP 分片和重组机制移除,不会造成通信质量下降和通信失败,而这样做不失一般性。

2)IP 头部数据结构精简

IP 数据帧选项字段主要用于网络测试或调试,正常通信时基本不用。因此,IP 选项可以移去。省去后的 IP 头部数据结构一共 20 个字节,对应的结构体如下:

```
typedef struct {
        byte vhl;                   //4 位版本,4 位首部长度
        tos;                        //8 位服务类型
        len[2];                     //16 位总长度
        ipid[2];                    //16 位标识
        ipoffset[2];                //3 位标志,13 位片偏移
        ttl;                        //8 位生成时间
        proto;                      //8 位协议
        word ipchksum;              //16 位首部检验和
        word srcipaddr[2];          //32 位源 IP 地址
        word destipaddr[2];         //32 位目的 IP 地址
        } ip_hdr;
```

其中,部分域可使用固定值填充,如标志字段固定为 010,片偏移固定为 0,表示

μLwIP 不支持 IP 数据帧的分段和重组;生存时间 TTL(Time to Live)固定为 7Fh,表示数据帧的最大生存时间;服务类型域各位都取为 0,表示普通服务质量。

2. IP 协议的实现

精简后的 IP 协议主要完成:①对接收的数据帧检验 IP 头部校验和;②对 IP 包封装和解封,并根据协议字段值将数据帧交给相应的上层协议。

1)接收过程

函数 Tiny_input()负责处理接收的数据帧,核对 IP 头部对应域的数值是否正确。如果正确,则根据协议字段的值交给相应的高层协议处理,否则丢弃该帧。程序流程如图 12.15 所示。为了节省代码空间,检查 IP 头部各字段值的软件编写统一采用 GOTO 语句。典型代码如下:

```
if(μLwIP_BUF - >vhl ! = 0x45)
  {
      goto ↓drop;
  }
drop:
  Tiny_len = 0;
  return;
```

2)发送过程

应用程序发送数据时,在帧头的各个域内填充相应的数值进行封帧,由 IP 调用"封帧和发送函数"发送到网络上。

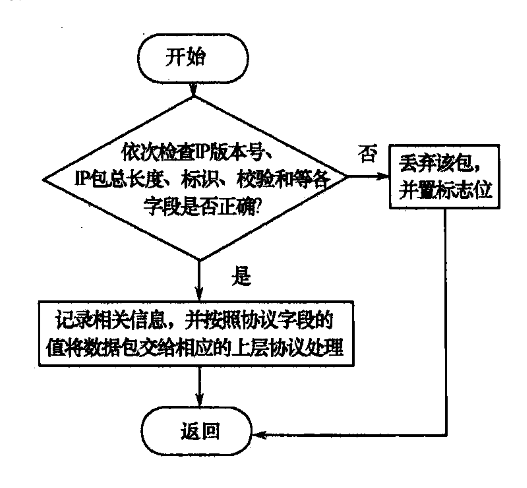
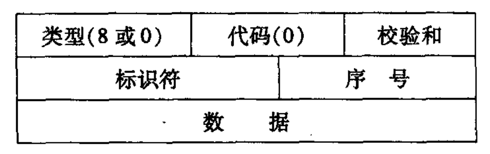


图 12.15　精简后 IP 数据帧接收流程

12.5.2.3　ICMP 协议的设计

本节只实现"ICMP echo 应答"一种类型的 ICMP 消息,用于 Ping 命令测试网络连通情况。Echo 请求和应答消息的代码都是 0,类型分别为 8 和 0。回送请求和应答 ICMP 帧如图 12.16 所示,标识符和序号用于匹配请求与应答(一台微机可以同时向若干个信宿机发出请求),μLwIP 只接收类型字段为 8 的 Echo 请求帧,并将类型字段 ICMP_ECHO 改为 ICMP_ECHO_REPLY,重新计算校验和回送给请求端,即除"类型和校验和"外,其他域保持不变。校验和的计算方法和 IP 头部校验和一样,但要计算整个 ICMP 消息帧(包括头

部和数据)的校验和。



类型(8 或 0)	代码(0)	校验和
标识符	序　号	
数　据		

图 12.16　ICMP 回送请求和回送应答帧格式

12.5.2.4　TCP 协议精简与优化设计

TCP 协议精简主要包括精简 TCP 状态机,减少同时支持的 TCP 连接数目;滑动窗口的精简;使用简单的重传机制。

1. 精简 TCP 状态机

面向连接和可靠性传输的特性决定了 TCP 每次通信都要经过 3 次握手建立和拆除连接,这个过程可以用状态机描述。为了状态机的正常工作,即各种状态之间的正确切换,必须存储每种状态的相关信息。状态机越复杂,TCP 协议实现的规模越大,维护状态机的开销就越多,对处理器存储能力的要求也越高。

因此,为不失一般性,本文采用图 12.17 精简的 Web 服务器状态机模型。将标准状态机客户端部分除去,精简了 Web 服务器关闭连接过程。

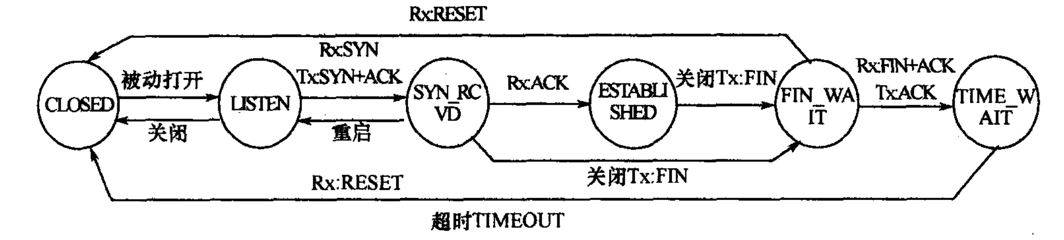


图 12.17　精简的 TCP 状态图

由于每个 TCP 连接由套接字唯一标识。Web 服务器接到客户端建立 TCP 连接的请求时,除了发送 SYN + ACK 以外,还要记录该 TCP 的状态,包括源端 IP 地址、源端口号、目的 IP 地址、目的端口号、序列号等大量连接信息,以便对接收和发送的 TCP 段进行跟踪。因此,本文基于节省存储开销的目的,使用较少的 TCP 状态数据,其连接状态结构体定义如下:

```
struct tcp_conn
{
    word ripaddr[2];      //远端 IP 地址
    word lport;           //本地端口号
    word rport;           //远端端口号
    byte rcv_nxt[4];      //期望收到的数据帧的序列号
    byte snd_nxt[4];      //上次被发送数据帧的序列号
    byte ack_nxt[4];      //下一个将被发送的数据帧的序列号
    byte tcpstateflags;   //TCP 状态与标志
    byte timer;           //重传定时器
    byte nrtx;            //重传次数
    byte mss;             //最大帧长度
```

```
    byte appstate[μLwIP_APPSTATE_SIZE];     //应用程序的状态
};
```

由于远程多用户访问 Sink 节点的页面，因此基于 LPC2210 和 IS61LV25616AL 的精简 TCP 支持多个 TCP 连接，目前可以实现 40 个连接同时存在。实践证明，这是合适的选择。

2. 精简滑动窗口机制

由于簇头节点处理了大量来自传感器节点的数据，因此递交给 Sink 节点的数据量并不大。Sink 节点在一次连接传输数据量不大的情况下，本文采用简单停等协议，即只使用一个滑动窗口，这样节约了系统的资源，方便维护。实际测试表明：实时性无明显的折扣，而且避免了流量和拥塞问题。

精简滑动窗口机制要求 Sink 节点也使用简单的确认机制[14]。如果 Sink 节点仍使用较大的窗口，本地处理器就可能被大量的数据“淹没”。因此，可通过合理设置“窗口大小”字段值，通知发送方自己的接收缓冲区大小，避免发送方连续发送大量数据造成接收缓冲区溢出，以至丢帧，同时使发送方也遵守同样的简单确认机制。

3. 应用层参与重传

超时重传是 TCP 的一个复杂算法，本文采用应用程序参与重传机制，对已发送的数据不作缓存。当重传计时器减至 0 时，激活 TCP 重传事务，然后调用 HTTP 回调函数 HTTP_APPCALL()，检测重传标志位，进行重传工作。如果在连接已经建立阶段，就重新生成重传数据；如果在连接建立或关闭过程中，说明丢失的是确认或应答帧，根据不同的 TCP 连接状态，重发不同类型的数据帧。这样并不会增加应用程序的复杂性，因为确认重传的时机是 TCP 的责任，而应用程序只需要使应用层数据指针重新指向上一次发送的数据，在数据量不大的情况下，不会对网络拥塞有明显的影响。

4. 精简 TCP 协议的实现

基于以上对 TCP 数据结构的分析以及协议机制的精简，大大降低了 TCP 协议的实现难度。图 12.18 描述了精简 TCP 协议的软件流程。

12.5.2.5　HTTP 协议精简与优化设计

只对以太网客户端的请求给予简单的响应，不作过多的解释，对于具有简单 Web 服务器特性的 Sink 节点是合理的。因此，没有必要实现完整的 HTTP 协议。

1. HTTP 协议的精简

1）请求帧精简

“对一个繁忙的服务器进行采样，统计结果表明：500,000 个客户程序的请求中有 99.68% 是 GET 请求，0.25% 是 HEAD 请求，0.07% 是 POST 请求。”因此，从嵌入式以太网角度来讲，在 μLwIP 的 HTTP 实现中，本文仅对 GET 请求给予响应。GET 请求帧格式为 GET /index.htm HTTP/1.0 <CR> <LF>，该帧仅包括请求行，根据请求行中的请求 URL 返回相应的文件。这样大大精简了 Sink 节点的响应过程，同样，也省略了 Web 服务器返回 HTTP 帧帧头，这样做并不违反 HTTP 帧的格式。

2）响应帧精简

对于响应代码，本文只实现两种：“200 OK 请求成功”和“404 没有找到”。当用户请求的文件找到时，发送“请求成功”帧头，反之，均返回错误帧头“没有找到”。因为对于特

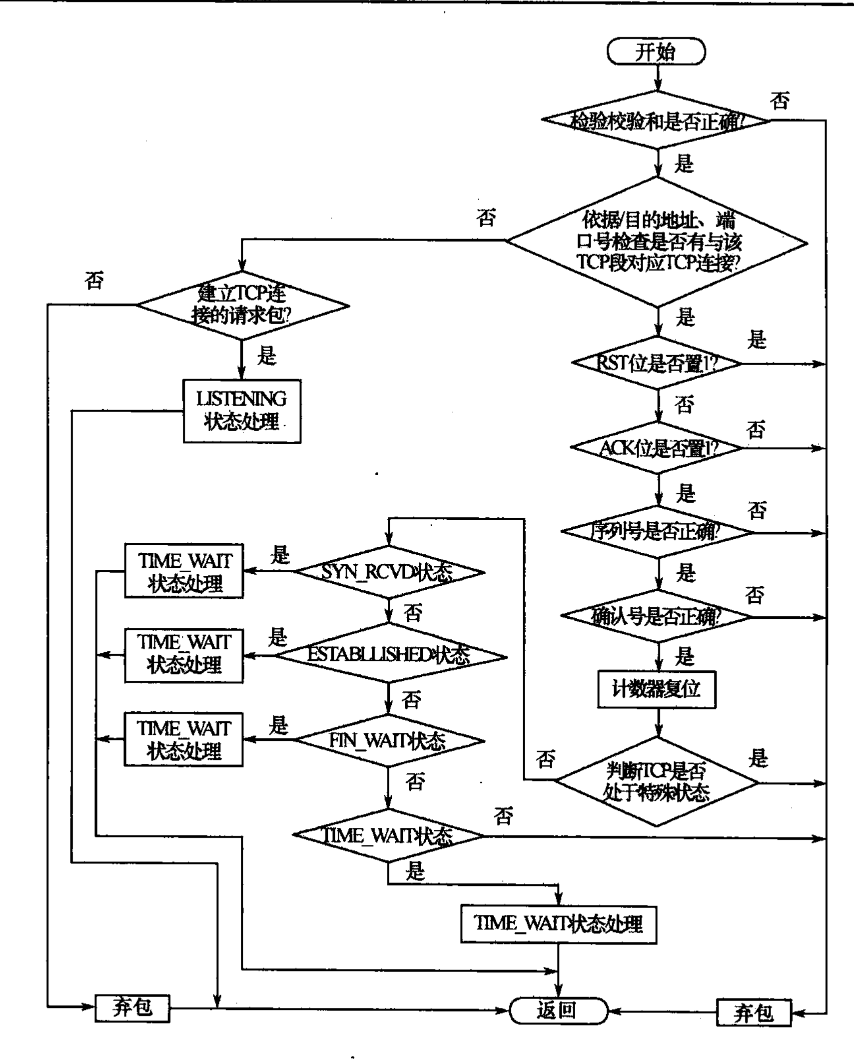


图 12.18　TCP 协议流程图

定的嵌入式应用，Web 服务器没有必要对响应出错做出过多的解释，尤其在 Sink 节点资源有限的情况下是合理的选择。

2. HTTP 协议的实现

协议的实现包括以下内容：

(1)根据测试函数返回值改变 Web 服务器状态。本设计定义了两个状态，即 HTTP_NOGET 和 HTTP_FILE。HTTP_NOGET 表明服务器和客户端建立连接后，还未接收到客户端发来的 GET 请求；HTTP 只是单纯地等待 GET 请求的到来。对于其他数据帧一概丢弃。

(2)对 GET 请求进行响应，返回所请求的数据。文件系统的目的是：当收到客户端的请求时，提供一条从服务器上存储的众多文件中找到所需页面的途径，μLwIP 用一个包含结构体指针的结构体查找文件。结构体定义如下：

```
struct fsdata_file_noconst
{
    struct fsdata_file *next;
```

```
        char *name;
        char *ddata;
        int len;
};
```

这个结构体将服务器存储的文件连接成一个链表。结构体指针 * next 指向链表的下一个文件首地址; * name 指向当前文件首地址; * ddata 指向当前文件实际数据首字节地址;len 存储数据长度。在这个结构体的基础上本文定义了 fs_open( )函数寻找目标文件。主要程序如下:

```
int fs_open(const char *name, struct fs_file *file)
{
    ..........
    struct fsdata_file_noconst *f;
    ..........
for ( f = (struct fsdata_file_noconst *)FS_ROOT;
      f != NULL;
      f = (struct fsdata_file_noconst *)f->next )
      {
            if(fs_strcmp(name, f->name) == 0)
             {
                 file->ddata = f->ddata;
                 file->len = f->len;
                 .....
                 return 1;
             }
      }
    return 0;
    .....
}
```

其中,const char * name 代表目标文件的名字,struct fs_file * file 指向找到的目标文件首地址。fs_strcmp( )是字符串对比函数,如果链表的某一文件名和目标文件名相同,说明客户端请求的文件存在,并将指针 * file 指向该文件返回 1。反之,如果找不到该文件,函数 fs_open( )返回 0。

12.5.3　μLwIP 的 Sink 节点嵌入与移植

1. μLwIP 接口

μLwIP 可看作是一个函数库,运行于物理层硬件基础之上,作为 μC/OS－II 的任务为 Web 服务器提供可靠、实时的通信保证。μLwIP 接口定义了 μLwIP、底层系统和应用程序之间的函数调用关系,如图 12.19 所示。

2. 应用程序接口

μLwIP 使用基于事件的程序模式,将应用程序实现为一个 C 函数,以减小程序的复杂性及时间与存储空间的开销。当任一事件发生时,应用程序 μLwIP_APPCALL( )将被调

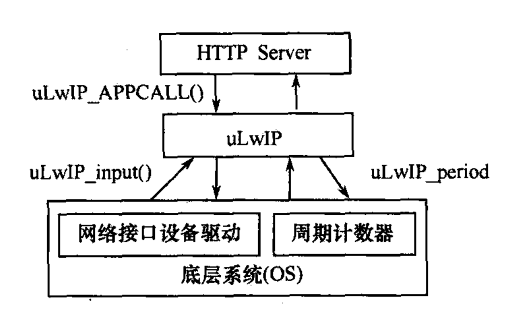


图 12.19　μLwIP 的接口模型

用。数据的接收、发送、新连接建立、重发等事件都需要调用应用程序。另外,应用程序也需要对端口进行周期性检测,检测是否有新的数据到来或需要发出,并负责把不同网络数据服务映射到不同的端口及连接上。

3. 操作系统接口

从操作系统角度,μLwIP 使用了 3 个函数:μLwIP_init( )、μLwIP_periodic( )和 μLwIP_input( )。μLwIP_init( )完成包括各种连接状态、缓冲区、变量、参数、端口等 μLwIP 的初始化。μLwIP_periodic( )周期性地被调用,用于驱动计数器和数据重传,当网络接口设备驱动将接收的数据放入接收缓冲区时,由 μLwIP_input( )负责处理。该函数返回一个非零值,说明服务器有数据要发送,且已放入发送缓冲区。

4. μLwIP 在 ARM 上的移植

根据上文分析,μLwIP 代码量小,移植性强,实现了 TCP/IP 协议族中的主要协议,基本满足嵌入式 Sink 节点的要求。但 μLwIP 是专门为 8/16 位微控制器设计的微型 TCP/IP 协议栈。而嵌入式 Sink 节点选用的是 32 位的 ARM 微控制器,因此,必须对 μLwIP 进行修改,使其适应 32 位微控制器的要求。本文从数据类型、数据存储结构及处理速度三方面进行修改。

在 μLwIP 中需要用到 32 位数据时,用两个 16 位的数据来代替。在图 12.20 中,结构体中成员变量 ripaddr[12]是包含 2 个元素的 16 位数组,代表客户端的 IP 地址。为了不影响处理速度,用 32 位数据 ripaddr 代替这个数组。

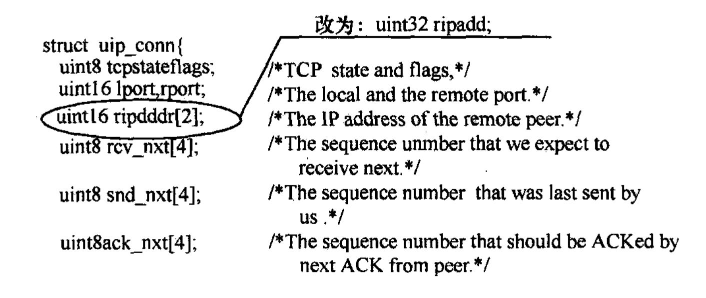


图 12.20　数据类型的修改

ARM7TDMI 体系结构中,Flash 数据存储必须以半字(16 位)对准。对于 32 位数据,要占两个半字的空间,对于 8 位数据,分以下两种情况,如图 12.21 所示。

(1)存放该字节(8 位)的物理地址为奇数。下一个数据无论是什么数据类型都按顺序从下一个物理地址(偶数地址)存起。

(2)存放该字节(8 位)的物理地址为偶数。下一个数据如果是字节型(8 位),就从下一个物理地址(奇数地址)存起;如果下一个数据是半字(16 位)或字(32 位)类型,则空出后面一个物理地址单元,从下一个偶数地址存起。

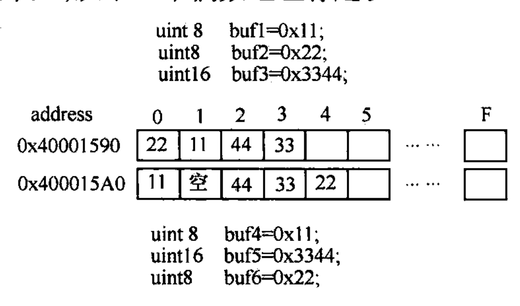


图 12.21　数据存储格式

在 32 位 ARM 上必须使用定时器延时,控制 TASK_μLwIPTimeOut( )任务中 μLwIP_periodic( )函数的执行,一般要等待周期性定时结束时才执行。

12.5.4　嵌入式 Web 服务器的实现

无线传感器网络和以太网的融合,将带来新的应用,一方面使传感器网络得以借助这两种网络传递信息,另一方面这两种网络可以利用传感信息实现应用的创新。

在上述嵌入式 TCP/IP 协议栈 μLwIP 的设计和实现的基础上,实现了一个嵌入式 Web 服务器。整个软件在 Keil μVision2 的环境下编译及调试通过,编译后的代码量约为 218.6KB。

本节设计的 μLwIP 协议组件包括 HTTP、TCP、IP、ICMP、ARP 协议等协议。HTTP 协议是网络通信平台和用户之间基本的通信传输协议,负责 Sink 节点与客户端之间的信息交互和解释。TCP 协议为其提供了一条可靠的数据通信链路。IP 协议屏蔽底层网络硬件细节,允许平台采用多种网络接口方式。ICMP 提供了简单的网络连通诊断。链路层协议 ARP 负责在点对点串行链路上传输 IP 数据帧。为了节省存储空间,IP、TCP 和 ICMP 协议可捆绑在一个函数 μLwIP_process( )中实现。基于 μLwIP 的嵌入式 Web 服务器数据处理流程框图如图 12.22 所示。

针对 μC/OS - Ⅱ操作系统,本文设计了 3 个任务模块:TASK_TinyRec、TASK_TinyTimeOut 和 TASK_TinyProcess。各任务函数基本功能及优先级如表 12.1 所列。其中,数据帧接收任务 TASK_TinyRec 优先级最高,保证了网络数据不会丢失;数据帧处理任务优先级最低,保证了其他任务的及时处理。软件系统用信号量进行任务的通信。这里只用了一个信号量,即 Sem_ProcessPackage(帧处理信号量)。

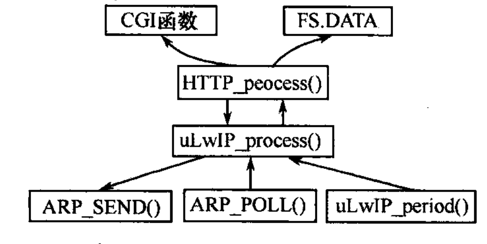


图 12.22　μLwIP 数据处理流程

表 12.1　嵌入式 Web 服务器任务设计

任　务	基本功能	优先级
TASK_TinyRec	接收网络数据帧	4
TASK_TinyTimeOut	处理网络数据帧	3
TASK_TinyProcess	超时询问	2

嵌入式 Web 服务器的工作流程如图 12.23 所示。协议栈初始化工作主要指对网络接口、TCP/IP 协议栈缓冲区、TCP 支持的协议端口号和连接状态等进行设置和复位。初始化后的服务器处于监听状态,一旦有浏览器的请求到达 80 端口,则建立连接。当接收到用户请求后,分解出 URL 和请求方法。如果是静态文本则直接读取并发送给浏览器;如是 CGI 脚本,则调用该脚本,完成数据采集或者执行控制指令。最后将脚本运行结果并返回浏览器,在一定时延后无后续请求则关闭该连接。

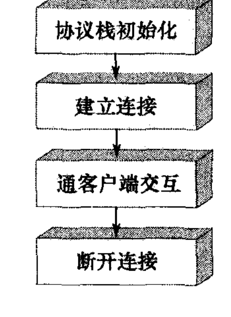


图 12.23　Web 服务器工作流程

Sink 节点的 Web 服务器仅对 80 端口开放,对于其他端口的请求一概丢弃,而且仅识别特定格式的用户请求和控制命令,相对于传统的大型服务器,其受恶意攻击的可能性很小,安全性较高。

12.5.5　Sink 节点动态网页和本地文件读写与保存的中间件

为了使传感器节点采集的数据经过 Sink 节点进入以太网后,在远端浏览器上实时刷新显示,动态网页支持是必要的。无线传感器网络的应用主要是远程智能监测,大量传感器节点采集大量的数据,但不作本地保存,而是实时上传,由于 Sink 节点需要对测量数据进行深度分析与处理,因此,采集数据的 Sink 节点本地保存和浏览器自动刷新数据十分必要。本文在 Web 服务器端采用 CGI(Common Gateway Interface)接口技术,以实现浏览器和 Web 服务器之间的交互;由于 Java 结构简单、数据传输代码量小、效率高,因此,采用 Java Applet 技术增强浏览器的功能,使浏览器可以实时刷新测量数据;采用数字签名技术,超越 Java 安全机制对大量数据进行本地保存;使用 C + + Builder 6.0 平台开发集中式监控软件中间件来实现监控数据的实时显示和动态更新。

Java 语言中 Applet 的运行机制是以组件形式嵌入网页,在 www 的浏览器/服务器环境下运行。执行过程中,在服务器一端的 Java 编译器把 Applet 源代码编译成字节码,在 HTML Script 中被调用;客户端是一个与 Java 兼容的浏览器,Applet 字节码在客户端被解释执行。这样 Applet 的运行不再受网络速度的影响,从而真正实现了网络通信上的动态交互性。

12.5.5.1　基于 CGI 接口的 Sink 节点动态网页

考虑到嵌入式 Sink 节点系统资源的限制,本小节采用 CGI 技术实现动态网页。CGI 程序属于一个外部程序,是运行在服务器端的一个可执行文件。CGI 和 Web 服务器与外部应用程序交互关系如图 12.24 所示。

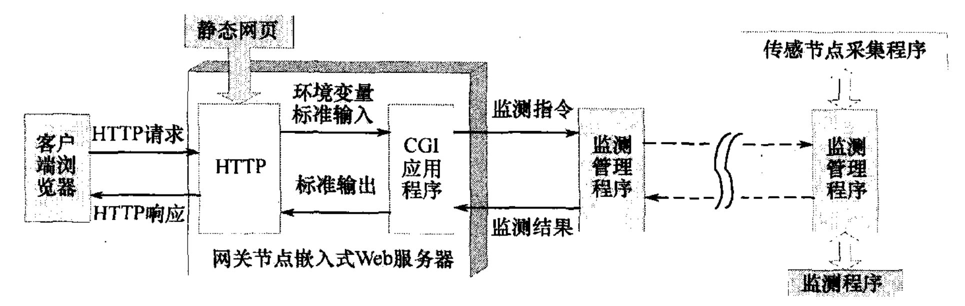


图 12.24　CGI、Web 服务器与外部应用程序交互关系

浏览器先将用户输入的指令或请求数据送到 Web 服务器，Web 服务器将数据使用 STDIN（标准输入）送给 CGI 程序，在执行了 CGI 程序后，使用 STDOUT（标准输出）以 HTML 形式输出 Sink 节点接收的数据，之后经 Web 服务器、浏览器显示给用户。

CGI 程序读入和输出数据的方式遵循 HTTP 协议的规则，但在处理数据阶段则无任何特殊限制。当用 CGI 实现远程数据采集和监测时，CGI 程序可以通过直接访问硬件或调用驱动程序的方式获得数据（本文采用调用驱动程序）。数据采集到后，CGI 程序将数据组织成 HTTP 流并发送到 Web 服务器，由 Web 服务器负责送到客户端。

由于 HTTP 是基于请求/响应模式的，一次采集请求只能得到一组数据，为了实现连续数据采集，本文采用建立 TCP 连接的方法[15]。

建立 TCP 连接就是通过在网页中嵌入 Java Applet 小程序增强客户端的功能。通过浏览器设定采样长度、采样频率等有关参数，并通过 GET 命令传给 Sink 节点内嵌的 Web 服务器；当 Web 服务器收到命令时，启动接收数据信号，把接收到的数据放到数据缓冲区中，如果接收到 DATA 指令，则和用户建立 TCP/IP 连接，将缓冲区的数据传送到用户端。这种方法的优点是不需要另外的客户端程序。实现监测数据的连续采集和实时刷新的 Applet 程序 MonitorApplet. java 如下：

```
try
    {
            URL u = new URL("http://202.117.87.18/TempData");
                    ……
            Thread.sleep(3000);
    }
```

将 MonitorApplet. java 编译后，生成 MonitorApplet. class 文件，在 HTML 代码中加入 <applet code = "MonitorApplet. class" width = 400 height = 200 > </applet>，就可将 Applet 嵌入到 HTML 页面中。

本文研究的 Sink 节点与以太网接入系统的浏览器端是 PC 机，可以安装与 Java 兼容的浏览器，容易满足 Java Applet 的运行机制；由 LPC2210 微控制器构成的 Sink 节点（微型网络服务器端）只具备简单的 TCP/IP 通信功能。将由字节码构成的 Class 文件放在微控制器的 Flash 中，通过 Sink 节点的嵌入式 Web 服务器程序便可实现对 Applet 访问和下载控制。

12.5.5.2　本地文件读写与保存的中间件设计

1. 本地文件读写的 Applet 程序

读写本地文件的 Applet 程序 RWFileApplet. class 主要包括向本地文件写入内容的 saveToFile 方法和读取本地文件的 loadFile 方法。具体实现过程如下：

1）saveToFile 方法

```
RandomAccessFile raf = new RandomAccessFile(filename,"rw");
raf.seek(0);                                      //将文件指针指向文件头
raf.writeBytes(fileArea.getText());               //将文本框中的内容写入文件
raf.close();                                      //关闭文件流
```

2）loadFile 方法

```
BufferedReader reader = new BufferedReader(new FileReader(fileName));
```

```
String content =new String();
while ((content =reader.readLine())! =null)
{
    fileArea.append(content +"/n");                    //逐行读取文件的内容
}
reader.close();
```

2. 本地文件保存的实现

本地文件保存的数字签名 Applet 开发和运行的过程如下：

(1)开发 Java 源程序 RWFileApplet. java,并对其进行编译,生成 RWFileApplet. class。

(2)用 JAR 工具对类文件 RWFileApplet. class 进行封装,生成 myClass. jar。

(3)用 keytool 创建密钥库文件 zn. store,生成 X. 509V1 签名证书,并输出证书文件 zn. cert。

(4)通过 jarsigner 工具用生成的密钥对 JAR 文件进行数字签名。

签名的 JAR 文件和 Class 文件一样,都是由字节码构成,可把它直接存放到微控制器 LPC2210 的 Flash 当中。

在浏览器端,除了安装 Java Plug - in 软件外,还需要定制 zn. policy 文件,修改\jdk1. 2\jre\lib\security\java. security 目录下的 java. security 文件。修改方法是在 java. security 文件中找到以下两行：

```
policy.url.1 = file:${java.home}/lib/security/java.policy
policy.url.2 = file:${user.home}/.java.policy
```

并添写第 3 行：

```
policy.url.3 = file:D:/work/javaapplet/testing/security/zn.policy
```

完成上述各步骤之后,就可以把远程传感器节点测量的大量数据采集到本地,并实现自动保存。

12.6　无线传感器网络接入网格

网格是构建在分布式资源和通信网络的物理基础上,以资源共享为主要方式,为用户提供按需服务的一种基础设施。它所提供的带宽、存储容量和计算处理能力几乎是无限的,并且能够支持资源之间的互操作,网格的这些特征能够很好地支持无线传感器网络的数据处理过程。为此,通过将无线传感器网络作为传感与信息采集的基础设施融合进网格体系,构建一种全新的基于无线传感器网络的传感器网格体系—无线传感器网格,使得传感器网络专注于探测和收集环境信息以及低层次的数据聚集。复杂的数据处理、存储和客户服务则交给网格来完成,从而通过网格平台有效驱动无线传感器网络智能化的自组织信息收集过程,为军事、科研和工商业等领域提供一个强大的用于数据感知、密集处理和海量存储的操作平台。

无线传感器网络接入网格后,具有以下诸多益处[16]：

(1)网格拥有的计算资源和存储资源可对无线传感器网络收集到的大量数据进行处理、分析和存储。

(2)同一个无线传感器网络所得数据可以通过网格平台同时被多个应用程序使用,

传感数据使用更加方便,数据使用率同时提高。

(3)在网格中可以利用数据挖掘、数据融合、分布式数据库等技术对其数据进行处理,获得传感数据的新知识。

12.6.1　相关研究工作及关键技术

目前,对无线传感器网络和网格计算已分别有了较深入的研究,但对将无线传感器网络融合进网格,以在更广阔复杂的背景下利用无线传感器网格来提升应用价值的意义认识得还很不够,对无线传感器网格方面关键技术的研究探讨也几乎没有,但可喜的是这方面的探索趋势正在逐渐形成。

美国哈佛大学提出 Hourglass 框架为异构的传感器网络提供网格 API,使用 SOAP 和与 Web 服务相关的协议支持交互,探索网络系统将每个传感节点作为一个网格服务与网格通信;但节点必须严重依赖于高性能的计算机,而无法做到低功耗和低成本。

Hourglass 主要由数据收集网络、传感器接入点和应用程序接入点 3 个部分构成。数据收集网络由一个互联网互联的系统构成,它能够发现、过滤、查询多个无线传感器网络。传感器接入点能够将应用程序的数据需求映射成底层的无线传感器网络上的操作,或者把无线传感器网络上的数据路由到数据收集网络。应用程序接入点是应用程序连接到应用程序接入点的连接系统,它将应用程序的请求映射到基于数据收集网络的服务上来处理。

SensorGrid[17]是将无线传感器网络和网格结合在一起构成的复合系统,它采用分布式网络结构,由传感节点、中间层和决策制定层构成。系统主要考虑了分布式数据融合、分布式处理、网络协同等问题,可以进行数据融合、事务监测和分类、分布式决策制定等工作。

无线传感器网络和网格是两个差异性很大的网络,两者在物理层、通信协议、应用协议等各方面都不同,两者在结合过程中遇到的网络连接、扩展性、任务调度等问题可以利用本书提出的结合框架来解决。

1. 不同网络连接问题

无线传感器网络中传感器节点之间的互联是通过低带宽、高延迟和不可靠的无线网络,传感器节点之间的无线连接会由于环境噪声和信号衰减的影响造成无线通信中断;网格中各种设备的互联是通过快速和可靠的有线网络。在结合框架中,需要解决传感器节点无线通信中不可预期的网络中断和通信延迟问题。

2. 无线传感器网络和网格的协议映射

网格通信中使用标准的因特网协议,如 TCP/IP、HTTP 等。无线传感器网络通信通常使用私有协议,尤其是 MAC 协议和无线路由协议大多都是私有协议。由于传感器节点的计算和存储能力有限,没有能力使用因特网协议,在结合框架中就需要将网格中使用的网络通信协议有效地映射到无线传感器网络的节点中。另外,网格的 OGSA 标准是基于 Web Service 的,它使用了 XML、SOAP 和 WSDL 等技术。让传感器节点将传感数据打包成 XML 格式并发布为网格服务是不现实的,需要结合框架将传感数据映射为网格服务。

3. 可扩展性

结合框架需要在不改变整体结构的前提下将无线传感器网络动态加入到网格中,它

要能够同时连接多个无线传感器网络，并可以容易地和网格的计算、存储资源进行集成，这样才可以使用户透明地使用多个无线传感器网络。

4. 能量管理

传感器节点使用电池供电，并且通常电量不可补充，能量管理是无线传感器网络中一个非常重要问题。从结合框架角度来看，传感器节点的可用性不仅取决于它们当前的负载状态，同样也取决于它们的能量剩余。结合框架应该能够提供适应性的能量管理服务，这样可以使使用无线传感器网络的应用程序在传感器节点操作和电量使用上找到平衡点。

5. 任务调度

无线传感器网络中，传感器节点的任务调度要考虑能量消耗和可用传感器资源。同时，无线传感器网络是以数据为中心的网络，在进行任务调度时，有效地利用传感器收集到的传感数据也是非常重要的一项工作。在结合框架中同时存在多个无线传感器网络时，要求调度过程能够充分利用多种类型的数据。

6. 系统安全问题

无线传感器网络所感知到的数据往往都是非常重要而且要求保密的，不允许任何数据的窃取和恶意修改，网格资源也要求经过认证的个人和服务提供者才能够访问。在网格中，通过认证和授权机制来确保访问者的合法身份，实现网格资源的安全访问。无线传感器网络通过使用节点认证、传感数据加密、安全 MAC 协议等方式来保证节电和传感数据的有效安全。结合框架为了同时保证网格和无线传感器网络的安全，需要将网格安全技术和无线传感器网络安全技术有机结合起来，确保整个系统的安全。

7. 健壮性

传感器节点使用电池供电、使用不可靠的无线通信网络通信，很有可能会造成运行在传感器节点上的传感任务失败。为了防止传感器节点上的传感任务失败，结合框架应该支持任务的复制和迁移。这样，如果部分传感器节点失效，传感任务也可以很快由失效传感节点迁移到正常节点。如果有足够的传感资源，传感任务也可以复制。这样，部分节点的失效不会影响到整个传感任务的执行。最后，如果传感任务被打断，在系统恢复后，传感任务应该能够从打断的地方重新开始。

8. 服务质量

服务质量可以决定系统是否能够提供有效的传感资源和服务。通过 QoS 参数可以规定网格传感任务所使用的传感器节点、存储空间、通信带宽、消耗电量等指标。通过这些指标的使用，可以增加传感任务的健壮性，避免节点失效和通信中断的影响。结合框架要满足不同 QoS 的需求，将从高层规定的 QoS 需求映射为底层的 QoS 参数。在传感任务需要多个不同的传感器资源时，为了达到要求的 QoS，需要对传感资源进行预留。

12.6.2　无线传感器网络接入网格的结合框架

为实现无线传感器网络与网格之间的互联互通，需要构建合适的接入平台将无线传感器网络融入网格体系，从而支撑起无线传感器网格的应用。该接入平台起到类似代理或网关的作用，具体来说需要具备以下特征要素：

(1)它是一个动态的、可重配置的软件结构。

(2)为网格提供通信代理,以与无线传感器网络进行通信。

(3)解析、转换、存储和管理传感数据,兼容不同类型的无线传感器网络。

(4)对无线传感器网络施加驱动。

(5)为多传感器网络之间的通信提供网关机制。

(6)提供标准的 Web 服务支持。

由于基于 OGSI(Open Grid Service Infrastructure)的方法引入了有状态的 Web 服务,同时也不支持通用的事件机制,这严重偏离了网格中 OGSA(Open Grid Service Architecture)框架的设计理念。而采用基于 WSRF(WS - Resource Framework)的机制构建这个接入平台,运用标准轻量级的无状态 Web 服务来管理传感器网络的状态资源,并将松耦合、异步的消息通知给应用客户,就能够有效地支撑起网格的 OGSA 框架实现。

根据上述分析的关键要素,把这种基于 WSRF 的具有解析、驱动能力并可融合多传感器网络的功能称作多解析驱动服务 MPAS(Multiple Parsing Actuating Service)。图 12.25 是使用 MPAS 接入平台将无线传感器网络接入网格的系统示意图。

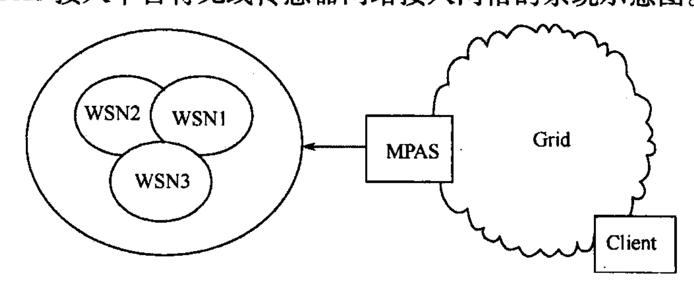


图 12.25　使用 MPAS 将无线传感器网络接入网格

进一步可以构建起由 MPAS 接入平台所支撑起来的无线传感器网格的体系架构:底层是无线传感器网络层,主要由传感器应用、节点应用和传感器网络应用构成,通过中间件连接节点,协调网络内服务,提供配置和管理整个网络的功能并进行有效的任务分配。接入层 MPAS 将不同类型的无线传感器网络平滑地接入到网格体系中,并协调管理传感数据信息资源。OGSA 层构建在 WSRF 所提供的 Web 服务基础上,用来实现网格平台中的核心服务(如名字解析、服务发现、安全策略等)、数据和信息服务、资源和服务管理。应用层提供系统开发工具和环境,并调用 OGSA 所提供的高阶服务。

MPAS 由 5 个基本组件构成,即通信机制(Communicator)、解析器(Parser)、WSRF 组件、驱动器(Actuator)和数据库(Database),这些组件之间具体的交互流程如图 12.26 所示。

1. 通信机制

将无线传感器网络接入网格中需要首先解决传感器网络和 MPAS 之间的通信问题。在通信的交互过程中,传感器网络和 MPAS 处于对等的地位,采用 P2P 的通信方式:传感器网络将收集到的信息送给 MPAS,MPAS 要监听这些传感信息并接收它们;MPAS 将驱动命令送给传感器网络,传感器网络也要监听并接收这些驱动信息,实现驱动功能。这样,通信过程中任何一方既要作为服务器来监听数据,也要作为客户端来发送数据。同时

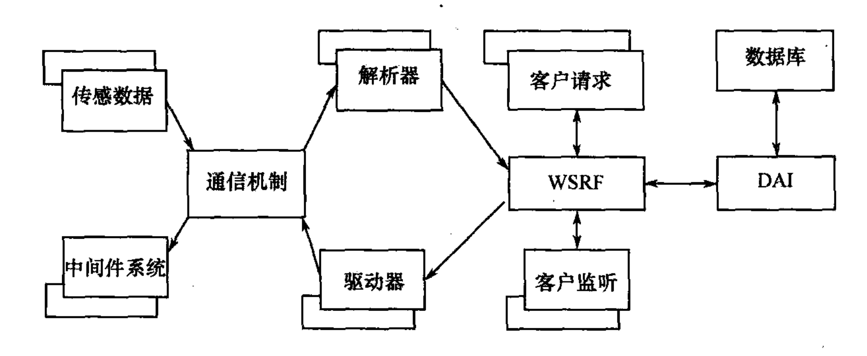


图 12.26　接入平台 MPAS 的交互流程

为了保证通信过程中的可靠性,要使用 TCP 的连接方式在传感器网络和 MPAS 之间建立面向连接的 Socket 通道,并使用 SSI,加密传输。

传感器网络与 MPAS 之间的通信流程如下:

(1)先在通信双方之间建立面向连接的 Socket 通道。

(2)初始化用来处理接收数据事务的会话池(Session Pool),使其处于就绪状态。

(3)双方各启动一个监听线程(TCP Listener thread)来监听 P2P 通信过程中的数据信息。在多传感器网络和 MPAS 通信的情况下监听到有数据信息到来时,如果会话池中存在着无状态接收会话实例,则立即激活其中的一个,并开始在这个会话实例中处理数据接收事务;如果没有,则立即创建一个无状态接收会话实例。

(4)接收完毕后,将此会话实例去除状态并送还到会话池中,等待下一次被激活使用。

2. 解析器

解析器使用 XML Schema 描述传感数据协议中所有的数据域,包括传感器网络的名字、各类传感数据、节点位置等。其主要功能是对传感数据流进行划分,提取出有效的传感信息,将其转化为网格中标准的传感资源。解析器的工作流程分为 3 步:

(1)使用 DTD 文件来定义 XML schema 的格式,并检查其合法性。

(2)解析器读取 XML Schema 将每个数据域细节分成名称、类型和长度信息,获得解析传感数据的格式。

(3)解析器在获取传感数据后,使用从 XML Schema 所得到的解析格式提取出相应的有效传感信息,并将其转换为统一的网格资源,送给 WSRF 组件处理。

通常传感数据是以十六进制的形式送入传感数据解析器的。在提取传感信息时传感数据解析器将比特作为分界点,以完全控制协议数据的每一个比特位,这样能够不浪费任何数据流带宽,无需对无线传感器网络的设计与实现作限制,也不需要修改现有的无线传感器网络协议,能够非常灵活地设计传感节点与网络特性。虽然使用解析器增加了 CPU 的运行负担,牺牲了 CPU 的效率,但最终能有效降低能耗,延长节点的寿命。

对于不同类型的无线传感器网络,通过修改其所对应的 XML schema 内数据域中对传感数据的描述,就能够有效兼容不同类型的传感器网络。这样,来自不同类型传感器网络的传感数据在经过解析器的处理之后,其信息表达模式对网格操作来说已经是一致的了,从而屏蔽了不同传感器网络的传感数据模式之间的差异。

3. WSRF 组件

WSRF 组件作为 MPAS 接入平台的核心，有机整合起解析器、驱动器、数据库和客户请求机制，并协调它们之间的交互行为。WSRF、组件的工作原理主要分为以下 3 个机制：

(1)通过与 MPAS 的其他组件交互来协调它们的行为。WSRF 组件从解析器获得传感资源，采用"推"的方式通过消息通知将它们送给订阅了相应主题的网格客户，将对传感器网络操作配置的请求转换成为语义上的驱动操作描述，送给驱动器去处理；使用 Database 组件的服务来操作分布式异构环境下的传感资源。

(2)使用 Web 服务操作有状态的传感资源。WSRF 组件的核心就是 Web 服务机制，它借助 WSRF 框架将传感资源抽象出来。网格客户则使用标准的 Web 服务来操作这些传感资源，首先 WSRF、框架对传感资源进行初始化，并登记主题事件，然后客户请求者使用 WSRF 框架中的 Web 服务来操作传感资源及其属性，最后销毁客户代理、Web 服务的实例、监听线程和服务管理者，结束交互。

(3)通知机制。WSRF 组件的通知机制采用 Publish/Subscribe 的模式，客户在 WSRF 中订阅相关主题的 Web 服务，并由一个专门负责服务订阅管理的 Web 服务来管理这些订阅过程。对于多传感器网络，WSRF 组件需要使用传感器网络的名字区分不同的传感器网络，即声明要接收哪个传感器网络的数据，然后向 WSRF 订阅相关主题服务，从而"拉动"WSRF 将数据送给相应主题的客户。多传感器网络环境下，WSRF 组件的事务处理流程如图 12.27 所示。

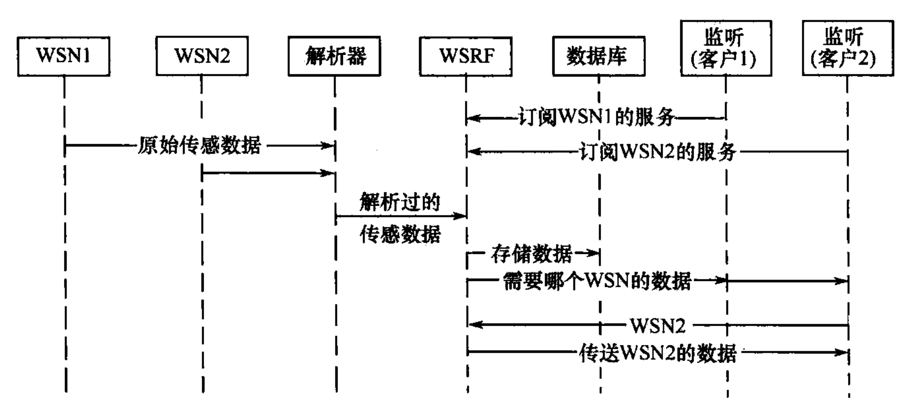


图 12.27　多传感器网络环境下 WSRF 组件的事务处理流程

4. 驱动器

无线传感器网络要进行初始化配置、分配任务以及调整自身的网络性能都需要接收来自外界的驱动。MPAS 中的驱动器就扮演这个"驱动者"的角色，对无线传感器网络施加驱动直接指导传感器网络的中间件系统完成这些部署、调整和任务分配的工作。具体的驱动流程如下：

(1)驱动器接收 WSRF 组件提交过来的对无线传感器网络进行操作配置的语义驱动描述。

(2)驱动器通过使用 XML Schema 来验证语义驱动描述是否符合事先约定的操作配置的语义规范。

(3)验证通过后，驱动器把语义驱动描述转换为能够操作无线传感器网络中间件系

统的命令机制，以指导完成对无线传感器网络的调整、优化、部署和任务分配等工作。

驱动器中的命令驱动者是一个十分关键的组件，它扮演"解析者"和"工厂"的双重角色，在解析语义驱动描述的过程中提取出对传感器网络的语义操作配置元素，并将资源和这些操作配置元素组装成能够操作传感器网络中间件系统的命令机制。这些命令机制由操作指令及相关配置参数组成，如 SELECT{fun{},attrs}、FROM sensors、WHERE {selPreds}、COST{cost limitation}、EPOCH DURATION。

5. 数据库

网格客户在 MPAS 中通过客户代理使用 OGSA－DAI 这个中间件系统以统一的方式来存取和管理异构环境下的这些传感数据资源，从而屏蔽了分布式异构数据源的差异，同时也有效共享了传感数据资源。

在与 OGSA-DAI 中间件系统交互的服务流程中，网格客户把对数据资源的操作以高阶服务的应用方式提交给 WSRF 框架中的 OGSA-DAI 服务，由 OGSA-DAI 服务的中间件进一步使用 DAI-Core 来具体地操作数据资源，最终实现以统一的方式存取和管理异构环境下的传感数据资源。对于多传感器网络，每一个传感器网络都在数据库中对应着一张数据表，当接收到来的传感数据时，根据传感器网络的名字将数据资源存放到所对应的表中。

参考文献

[1] 中国计算机学会. 中国计算机科学技术发展报告 2007[C]. 北京:清华大学出版社,2008:384－411.

[2] Wanner L F, Junior A S H, Polpeta F V. Operating System Support for Handling Heterogeneityin Wireless Sensor Networks. In 10th IEEE International Conference on Emerging Technologies and Factory Automation, Catania, Italy, Sept. 2005.

[3] 段渭军,何戟,张倩. 无线传感器网络移动 Sink 网关系统的设计与实现[J]. 计算机应用研究. 2007, 24(3): 241－243.

[4] 欧杰峰,刘兴华. 基于 CDMA 模块的无线传感器网络网关的实现[J]. 计算机工程,2007,33(1): 115－117.

[5] 匡兴红,邵惠鹤. 无线传感器网络网关研究[J]. 计算机工程, 2007,33(33): 228－230.

[6] Marco, Bhaskar K. Integrating future large-scale wireless sensor networks with the Intemet[J]. DePartment of Eleetrical Engineering University of Southern Califonia Los Angeles, March 2003: 86－91.

[7] 李金梁. 嵌入式 Internet 通信平台设计与实现[D]. 西安:空军工程大学,2005.

[8] 孙勇. 分簇型无线传感器网络关键技术研究[D]. 西安:空军工程大学,2008.

[9] 吴玉田,王瑞光,等. GSM 模块 TC35 及其应用[J]. 计算机测量与控制,2002,10:79－82.

[10] 张正红,胡小军,等. 基于 GSM 短消息接口的 MC3 一体化遥测系统[J]. 单片机与嵌入式系统应用,2003,3: 99－104.

[11]张劼,景博,张宗麟,等. 基于嵌入式 Web Server 的无线传感器网络系统设计[J]. 传感技术学报, 2006,19(2): 468－472.

[12] 王勇,陈抗生. 嵌入式 Internet 中的协议选择[J]. 电信科学, 2004.4.

[13] Adam Dunkels. LwIP 0.9 protocol stack[EB/OL]. http://www.sics.se/～adam, 2003.4.

[14] 王勇. 嵌入式 Internet 的技术实现及其安全问题的研究[D]. 杭州:浙江大学, 2002.

[15] 中国计算机学会. 全国第五届嵌入式系统学术交流会论文集. 北京. 2004.

[16] Mark Gaynor, Steve Moulton. Integrating Wireless Sensor Networks with the Grid[J]. IEEE Internet Computing, 2004, 7:32－39.

[17] Chen-Khong Tham, Rajkumar Buyya. SensorGrid: Integrating Sensor Networks and Grid Computing[J]. CSI Communications, 2005, 7(29): 24－29.

第 13 章　无线传感器网络 QoS 技术

无线传感器网络的服务质量(Quantity of Service,QoS)技术是当前无线传感器网络研究的一个热点,在无线传感器网络的某些应用中,必须考虑到网络系统服务质量的支持问题。例如,在战地环境中,定位、探测和识别一个移动目标时需要用到图像/视频传感器,传感器节点和控制者之间需要进行实时数据的交换,以便采取相应正确的行动。因此,如何对这些有特殊需求的流量进行 QoS 保证是一个不容忽视的技术问题。

本章从无线传感器网络的 QoS 需求入手,首先讨论了在无线传感器网络中研究 QoS 的必要性,由于无线传感器网络是面向应用的网络,针对不同的应用 QoS 有着不同的含义和需求;其次在网络层面上分析了无线传感器网络 QoS 的特点,说明其与传统网络的区别,并且说明了无线传感器网络中 QoS 的研究现状、方法和面临的挑战;详细介绍了能源管理、覆盖控制、数据融合以及拥塞控制等方面的若干关键技术,给出了研究 QoS 的一些评价指标;最后从路由协议、跨层设计、中间件技术、动态资源管理、确保实时业务等方面描述了 QoS 的保障机制。

13.1　无线传感器网络 QoS 概述

13.1.1　传统数据网络 QoS 技术

有线网络一般通过资源的超额供应或网络流量控制来获得 QoS 支持。超额供应是通过增加冗余的网络资源来向有带宽需求的多媒体业务提供满意的服务,这种方法易于实现,但由于所有的用户都在一个服务等级,在流量达到高峰时,服务可能变得不可预测。而在基于流量控制的方式中,业务可分成不同的服务等级,每个等级有不同的优先级。

目前有两种基于流量控制来获得 QoS 的途径,即基于预留的方式和非预留的方式。基于预留的方式依据带宽管理策略以及业务的 QoS 需求来分配网络资源,如因特网的 IntServ(集成服务)模型。集成服务的基本思想是在传送数据之前,根据业务的 QoS 需求进行网络资源预留,其核心是 RSVP(Resource Reservation Protocol)协议。该协议是一种信令协议,用于通知网络中传输业务数据流的每一个节点来预留资源,如果资源预留失败,则会向主机发回拒绝消息。基于资源预留的集成服务对网络中路由器的存储能力和处理能力要求都很高,预留资源中所占用的开销大,可扩展性很差。而非预留的方式无需预留网络资源,它是通过一些策略如接纳控制、策略配置、流量分类、队列机制等来获得 QoS。接纳控制机制负责在节点流量的入口处控制流量能否接入网络,并且保证被允许接入网络的流量的 QoS 需求;策略配置确保没有节点违反预先为其分配的服务等级;流量分类区分数据包的优先级并由此获得在每个中间节点上每一跳的具体行为;队列机制

负责在发生拥塞时丢弃低优先级的数据包。

有基础设施的无线网络，如无线局域网和宽带无线接入网是有线网络的扩展，一个通信单元的所有移动主机都能在一跳之内到达一个基站，此时 QoS 问题主要来自于带宽的不足和用户移动的复杂度。所以可将有线网络中的 QoS 体系结构和无线 MAC 协议结合起来，无线 MAC 协议提供不同等级的数据流量，以不同的优先权接入共享无线媒介，从而获得全局 QoS 支持。虽然有基础设施支持的移动网络可以通过基础设施如基站和中心节点进行集中控制和管理，但如何实现基础设施之间的平滑切换和移动主机的无缝通信问题是其面临的主要技术难点，目前已提出包括小区切换机制和移动 IP 在内的大量协议和相关技术。

13.1.2　Ad Hoc 网络 QoS 技术

无线 Ad Hoc 网络是一个移动的自组织多跳网络，随着信息技术的迅速发展、多媒体应用的不断开展以及需要与其他网络进行互联，人们自然要求在 Ad Hoc 网络上能够传送综合业务，并希望能像固定的有线网络或蜂窝无线网络一样为不同业务的服务质量提供保障。

无线 Ad Hoc 网络与传统有线网络和有基础设施支持的移动网络不同，它的网络拓扑经常发生变化，带宽、能量和存储计算能力受限。因此，原本在有线网络中运用的没有考虑移动性 QoS 支持机制和许多无线网络中没有考虑多跳情况的 QoS 保障机制都无法直接应用。

Ad Hoc 网络中的服务质量保证是个复杂的系统性问题，它意味着需要提供"质量可以接受的信道"，支持 QoS 的信道接入协议，识别能够满足业务量要求的转发节点及在节点实施拥塞控制和管理。无线 Ad Hoc 网络的服务质量保障机制结构如图 13.1 所示，包括系统 QoS 模型、QoS 指令系统、QoS 路由算法以及 QoS－MAC 算法。

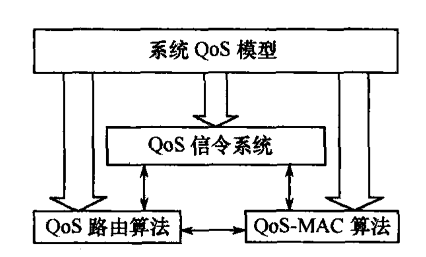


图 13.1　Ad Hoc 网络 QoS 保障机制结构

系统 QoS 模型指出保障机制所采用的体系结构，定义了网络中为用户提供各种业务的质量标准和等级，标志最终应该达到的系统设计目标。系统 QoS 模型影响着 QoS 其他构成部分的功能，如网络只需提供区分服务时，每个业务流状态的信令就不再需要。

QoS 信令是业务服务质量的控制中心，包括当前网络无线资源信息的收集、计算、分配、预留和释放，各个用户间业务请求的应答、调度等功能，同时协调 QoS-MAC 和 QoS 路由算法。

QoS 路由算法负责在网络中搜索满足信令系统给出的服务质量要求的从源节点到目的节点的路径。

QoS-MAC 算法则根据协议确定的数据传输任务，完成相邻节点间的最终数据传递。它能否高效地使用无线信道是上层各种协议和机制所提供的 QoS 能否得到最终保障的一个关键因素。

总之，在无线 Ad Hoc 网络的 QoS 保障机制中，QoS-MAC 算法、QoS 路由算法和 QoS 信令系统相互配合，共同实现网络 QoS 模型中定义的业务服务质量控制保障。

无线传感器网络中，由于传感器节点的能源十分有限，如果节点因能量很快耗尽而失效或者网络中各节点能耗不均衡，就容易使网络中出现感知黑洞，甚至极大地缩短网络生命周期。所以，在设计无线传感器网络时，首先要考虑如何节能的问题，即网络能量有效使用问题，但在某些类型的传感器网络应用中，必须重点考虑到 QoS 支持的问题。

QoS 这一术语不仅在传统的电信领域里得到了广泛使用，还逐渐扩展应用于基于分组的宽带、无线和多媒体等服务领域。与此同时，通信网络和通信系统的设计和规划也越来越多地考虑到用户应用端到端的性能需求。有关 QoS 的有效定义，ITU-T 标准化组织在 E. 800 中是这样描述的："QoS 是一种服务性能的综合体现，这种服务性能决定了网络在多大程度上满足业务用户的要求。"具体而言，QoS 是指网络为用户提供的一组可以测量的预定义的服务参数，包括时延、时延抖动、带宽和分组丢失率等，也可看成是用户和网络达成的需要双方遵守的协定。从根本意义来说，QoS 指的是网络对业务性能要求的支持能力。这里的性能要求是特定于不同业务的，如 IP 电话要求有尽可能小的抖动和时延性能，而远程医疗则需注重业务提交的准确性与重要性。

根据使用含义的不同，QoS 可以从两个不同的视角来解释。从用户角度来说，QoS 一般指用户所感知的业务的服务质量水平，用户并不关心网络内部设计的细节问题，他们只关心最终能够获得的网络提供的服务质量；而从网络角度来说，QoS 是网络提供给用户的服务质量水平量度，网络的目标是在提供 QoS 的同时，最大化利用网络的资源，即获得更加确定的通信行为，以便能够更加安全可靠地保护网络承载的信息，并更加高效地使用网络资源。为了达到这个目标，网络必须能分析各种应用需求并采用相应不同的 QoS 机制。

网络提供特定 QoS 能力依赖于网络自身及其采用的网络协议的特性。对于传输链路而言，包括链路时延、吞吐量、丢失率和出错率；对于网络节点而言，包括处理速率和内存空间等。此外，运行在网络各层的各种 QoS 控制算法也会影响网络的 QoS 支持能力。

13.1.3　无线传感器网络 QoS 需求

无线传感器网络作为无线自组织网络中的一个新成员，有自身特征和需求，并从根本上区别于传统的网络，主要原因有两点：一是其采用的网络器件是微型传感器，这些传感器节点的能量、处理能力和容量都十分有限，同时节点密集分布在偏远恶劣的环境中，节点失效和因节能休眠会带来复杂且动态的拓扑；二是网络中的业务需要的并不仅仅是通信，还涉及到感知信息的采集及产生、数据的协同处理以及信息的网内存储和直接转发等。这些都给无线传感器网络中的 QoS 支持增加了复杂度。

无线传感器网络可以有很多应用，它们的 QoS 需求也有很大的不同，针对不同业务，需要不同的 QoS 支持的解决方法以适用于每种应用。

QoS 可以从不同的角度以不同的方式来解释。由于 QoS 需求受网络中业务的影响，首先可以不从网络视角而是从其他视角来定义 QoS。例如，在事件探测和目标跟踪业务中，探测的失败或者获取事件信息出错可能来自于多个原因：可能是因为传感器播撒或网络安排的不妥当，即在事件发生的区域没有任何激活的传感器，因此直观上可以定义激活的传感器的覆盖范围或者数量作为衡量无线传感器网络中 QoS 的参数；或者，上述错误也可能来由于传感器的功能受限，如观测精度的不足或数据传输速率较低，因此也可以定义观测精度或是测量误差作为衡量 QoS 的参数；此外，问题还有可能是传输过程中信息的丢失引起的，进而也可以相应定义一些与信息传输相关的参数来衡量 QoS。

然而，对 QoS 视角的分割不是绝对的，一个普通的业务需求，如与事件探测相关的性能度量很有可能涉及到上述全部原因，还要把重点放在基础网络怎样向业务提供 QoS 这个问题上，包括信息的处理和传输、用哪些参数可以将业务需求映射到网络基础结构上，并相应地来衡量 QoS 支持。

下面描述无线传感器网络中 QoS 的两个观察视角：

(1)特定业务 QoS。从这个视角，可以考虑以下几个 QoS 参数，如 Active 传感器的覆盖范围、传感器位置排列、测量误差以及激活传感器的最佳数量[5,6]。简要说来，业务对传感器的布置、激活传感器的数量、传感器的测量精度等都有特定的要求，这些和业务的质量有着直接的联系。

(2)网络 QoS。从这个视角，考虑基础通信网络怎样才能传输有 QoS 限制的感知数据，并且能够有效地利用网络资源。虽然不可能分析无线传感器网络中所有设想的业务，但可以根据不同的数据传输模式来分析各个不同类型的业务，因为每种类型中的大部分业务都有共同的需求。从网络 QoS 的视角来看，在无线传感器网络中，关心的是数据怎样传输给 Sink 以及由业务特性所决定的相应的一些处理和传输的需求。

下面简要分析一些无线传感器网络典型应用，如环境监测、目标视频跟踪和分布式存储等的 QoS 需求。应用层的 QoS 需求是由用户指定的，如系统寿命、响应时间、数据更新度、检测概率、数据保真度和数据精度等。然而，用户的 QoS 需求往往会存在某些矛盾冲突，即改善和满足用户一个 QoS 需求的同时，会恶化或降低满足另外一个用户的 QoS 需求的能力，因此，需要网络设计者来平衡和调节。例如，给定相同的物理层射频 RF 单元，在 MAC 改善传输可靠性的同时会恶化有效节能，因为带来了重传、确认以及纠错编码等能量开销。

无线传感器网络与应用相关的 QoS 需求还有覆盖、暴露、测量差错，以及最优激活的节点数目等。与网络相关的 QoS 需求主要是解决以下 3 个问题：

(1)底层的网络如何有效地利用网络资源传输 QoS 约束的传感器数据。

(2)通过数据传输模型分析每一类应用。

(3)选择数据传输的模型，如事件驱动、查询驱动以及连续传输模型等。

注意到无线传感器网络与传统数据网络 QoS 需求的差别，无线传感器网络不再是端到端的应用，因此，QoS 参数都是集体参数，如集体延迟、集体分组丢失、集体带宽以及信息的吞吐率等；带宽并非是单个传感器节点主要关注的目标，或许一群传感器节点才会关注带宽。可以容忍单个节点产生的业务分组丢失到一定程度，大多数无线传感器网络应用都是任务紧急的应用，对延迟有较高要求。

13.1.4　无线传感器网络QoS特点

通常,QoS具有两方面的含义:一是从应用的角度看,QoS代表用户对于网络所提供服务的满意程度;二是从网络的角度来看,QoS代表网络向用户所提供的业务参数指标。为了方便分析,人们将无线传感器网络的QoS分为两个层面,分别是针对用户的应用层面和针对服务的网络层面。本节着重从网络层面介绍无线传感器网络QoS的特点。

从网络的观点来看,人们所关心的不是实际执行的应用程序,而是在有效利用网络资源时,下层通信网络如何发送数据给Sink节点以及该过程相关的需求。可以根据数据发送模型对无线传感器网络的应用进行分类,每个类别中的多数应用程序对QoS都有共同的需求。通常来看,可以分成3种基本数据发送模型,分别是事务驱动模型、查询驱动模型以及连续传输模型。

1. 事件驱动模型

当网络监测到某一事件发生时,目标附近的节点将立即处于激活状态,将采集到的数据传送给Sink以便通告最终用户,如针对某幢大楼化学元素释放的紧急事件进行感知和反应。

事件驱动模型的QoS需求有以下特点:

(1)应用程序本身并不是端到端的,具体地说,应用程序的一端是Sink,但另一端并非单个传感器节点,而是受事件影响的某一区域内的若干传感器节点。

(2)来自这些传感器节点的数据很可能具有高度关联性,因此包含大量的需要整理提取的冗余信息。

(3)虽然由单个节点发出的数据流量强度可能非常低,但是事件突发时,大量的节点将产生突发的大流量,网络要保障流量的可达性。

(4)一旦侦查到事件,应用程序必须尽快且可靠地做出恰当的反应,因此其对实时性要求较高。

(5)该模型的应用必须是可交互的。

(6)事件驱动模型通常具有关键性,要求重要信息具有较高的可靠性。

2. 查询驱动模型

在查询型网络应用中,首先由应用程序或者终端用户发出感兴趣的查询消息,之后,传感器节点将符合查询条件的数据逐跳转发至Sink节点。

查询驱动模型与事件驱动模型的区别在于,前者是通过Sink来请求数据,而后者是传感器节点主动将数据发送给Sink。这里所提到的"查询"也可能包含针对传感器节点的配置和管理信息。如果Sink想升级传感器节点的软件,重新配置发送速率,或者改变节点的任务,则Sink可发送一个指令来执行这些任务。

查询驱动模型的QoS需求类似于事件驱动模型,其同样是非端到端的程序,具有高度数据冗余、易产生突发的大流量、必须是可交互的,且具有关键性。查询驱动模型对于时延的容忍性根据具体的应用而有所不同。此外,由于Sink发出的指令是单方向的流量,因此要求较高的可靠性。

3. 连续传输模型

在连续传输模型中,节点不断采集数据,并以预先设定好的速率向Sink发送数据。

该模型的数据包括实时和非实时两种。实时的数据包括话音、图像和视频等；而非实时的数据可能是 Sink 在一定区域内周期性收集的数据。

对于 QoS 需求，连续传输模型是非端到端的程序，具有关键性，其应用可以是非交互性的。此外，不同的数据类型也有不同的 QoS 需求：实时的数据受限于时延，且有确定的带宽需求；而非实时的数据可以容许一定的时延和数据包丢失。

文献[1]中指出，QoS 是网络将用户数据从源端传到目的端的过程中必须满足的一系列的服务需求。不同的应用有不同的 QoS 要求，它为用户提供了一组可以测量的预定义的服务参数，包括如时延、时延抖动、带宽和分组丢失率等。

无线传感器网络是与应用相关的网络，这种同应用相关的设计方式的优点是能够对网络和节点软硬件资源，根据不同应用的要求最大限度地进行优化；缺点在于网络软件、硬件、拓扑、结构和路由等，在不同应用下有不同的表现形式，每种应用对 QoS 的要求也不尽相同。

表 13.1 概括了 3 种应用类型对不同性能参数的要求，可见无线传感器网络所保障的 QoS 不再是传统网络中端到端的概念，带宽和丢包率也不再是单个传感器节点所关注的主要目标，而是在特定时刻内一组传感器节点突发性传输数据所必需的服务质量，这种保障强调以任务的关键性为中心。

表 13.1　不同数据发送模型的性能需求

业务种类	基于事件驱动	基于查询驱动	基于连续驱动
端到端(End-to-End)	否	否	否
交互性(Interactivity)	需要	需要	需要
容许一定时延(Characteristics)	不容许	具体设定	容许
任务的关键性(Criticality)	是	是	是

4. 混合型

在很多应用中，上述数据传输模式同时存在于网络中。因此，需要有一个机制来适应有不同 QoS 限制的流量类型。

从表 13.1 可以看出，无线传感器网络中的业务需求和传统网络有许多不同。首先，传感器网络中的大多数业务不再是传统的端到端业务，而是“event-to-Sink”业务；其次，对于单个传感器节点，带宽并不是主要关心的，但对于一组传感器节点在某个特定的时间周期内，带宽是需要着重考虑的，这归因于传感器流量的突发特性；再次，因为冗余数据的存在，所以容许流量中由一个传感器节点产生的特定程度的丢包率；最后，无线传感器网络中的很多业务都是重要业务，都有很高的优先级。

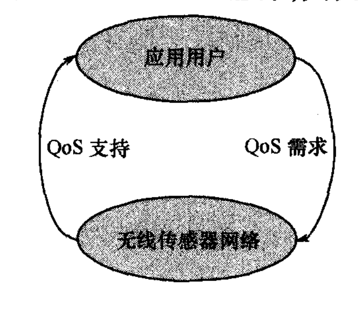


图 13.2　一个简单的 QoS 模型

D. Chen 和 P. K 提出了一个最简单的无线传感器网络 QoS 模型，如图 13.2 所示。该模型实质上就是网络和用户的 QoS 信息的交互模型，网络为用户提供 QoS 支持，而用户给网络提出 QoS 需求。由于网络体系结构中每个层次都有不同的 QoS 需求，如 MAC 层需要物理层提供信道的信噪比以确定选择哪个质量较佳的信道进行用户接入和传输。网络层需要 MAC 提供信道的使用情况，以决定选择哪条

业务最不拥塞的路径路由数据。传输层也需要网络和MAC层的状态信息,以便满足用户的传输差错率需求。因此,根据用户具体应用的不同,恰当地选择合适的QoS保证机制,是无线传感器网络QoS保证技术未来研究的主要课题。

在设计无线传感器网络QoS保证机制时,不但要考虑来自用户应用的需求,还要对系统网络的特点和结构做深入的分析。表13.2给出了设计无线传感器网络QoS保证机制应当考虑的主要因素。此外,在处理无线传感器网络的QoS业务时,还应该注意以下几个方面:网络带宽的限制、消除冗余数据传输、能量和延迟的平衡、点缓存大小的限制和多业务类型的支持。

表13.2　设计QoS保证机制应考虑的因素

问题	考虑的主要因素
网络的动态变化	包括传感器节点、目标跟踪和Sink节点的移动性
数据传输模型	连续模型、事件驱动模型、查询驱动模型、混合传输模型
数据汇聚、融合	在网内(部分或完全方式)或网外汇聚或融合处理
节点通信	单跳、多跳、单跳—多跳相结合
节点功能	多种或单一功能;同构或异构功能
节点部署、配置	按照预先规划的或以AdHoc自组织方式

无线传感器网络QoS的支持不仅包括QoS保证机制,而且还应当包括QoS控制机制。Ranjit Iyer和Leonard Kleinrock针对无线传感器网络的QoS控制问题提出了QoS的反馈机制和传感器网络的融合策略,将无线传感器网络的QoS定义为平均传感器网络精度,即向信息收集的汇聚节点发送信息的最优的传感器节点数目。换言之,如果网络节点数目太少,就不能保证传感器节点采集信息的精度;如果节点数目太多,又不能实现最小化能量的使用。其核心思想就是允许基站利用一个广播信道将QoS信息发送给每个传感器节点,并且运用了一个称为GurGame的数学优化方法来动态调节最优的传感器数目。这样,基站就可以根据变化的环境动态调节来自于传感器节点的QoS的精度。

13.1.5　无线传感器网络QoS研究现状

目前,国内外研究人员在多个方面和不同层次对无线传感器网络的QoS保障问题进行了研究,取得了一些有价值的探讨和研究结果,表13.3对QoS研究状况进行了总结。

表13.3　QoS研究现状

研究角度	思　路	特　点	典型代表
传统端到端的QoS	沿用传统IP网络中端到端QoS要求,建立满足QoS约束条件的路由	对实时业务提供一定的QoS支持,但协议实施复杂,开销大,不满足能量有效性	文献[2][3]
保障传输的可靠性	考虑链路和信道的多变情况,根据业务的优先级采用可靠的传输路径,并实施拥塞控制	提出非端到端的概念,基于可靠性和节能要求保障QoS,但缺少对其他QoS参数的考虑	文献[4]
与节点问题相关联	将QoS问题具体到监测区域内传感器节点数目的优化,如何最大程度地满足覆盖目标,调度传输节点	对QoS的支持仅从节点的角度来定义,还需要扩展到网络的层面	文献[5][6]

由此可以看出，由于研究的角度不同，对无线传感器网络中 QoS 问题的理解也存在差异，为更好地解决 QoS 问题，需要结合不同应用类型的特点来进行深入的分析[9]。

研究无线传感器网络 QoS 的方法较多，总结起来大致有以下几种：

（1）简化 QoS 模型。QoS 目前被分为两大服务类型，即集成服务类型（InterServ）和区分服务类型（DiffServ）。集成服务是指在整个网络中为某一业务流量保留一定的带宽，为该业务提供一条端到端的透明通道。集成服务的基本思想是在传送数据之前，根据业务的 QoS 需求进行网络资源预留，从而为该数据流提供端到端的 QoS 保证。集成服务能够在 IP 网上提供端到端的 QoS 保证。但集成服务对路由器的要求很高，当网络中的数据流数量很大时，路由器的存储和处理能力会遇到很大的压力。因此，集成服务可扩展性很差，难以在因特网核心网络实施，目前业界普遍认为集成服务有可能会应用在网络的边缘上。区分服务定义了一种可以在互联网上实施可扩展的服务分类，是一种基于每一跳的 QoS 策略。区分服务的基本思想是将用户的数据流按照服务质量要求来划分等级，任何用户的数据流都可以自由进入网络，但是当网络出现拥塞时，级别高的数据流在排队和占用资源时比级别低的数据流有更高的优先权。区分服务只承诺相对的服务质量，而不对任何用户承诺具体的服务质量指标。区分服务模型和集成服务模型由于它们的复杂性而不适用于无线传感器网络，跨层思想可能会比传统的分层更有助于设计一个简单的 QoS 模型。

（2）区分服务。区分的标准有很多，可以基于流量类型、数据传输模式、传感器类型、应用业务类型以及包的容量，如何根据业务需要合理地进行流量区分，如何控制不同类型流量的网络资源分配以获得最大的资源利用。

（3）自适应 QoS 保证算法。希望在整个网络生命周期内都能获得 QoS，而不是仅仅得到一个随时间推移而慢慢衰退的质量，因此需要一些自适应的 QoS 算法来防范网络拓扑动态变化对 QoS 保证的影响。

（4）QoS 支持集成化。需要研究怎样将无线传感器网络和基于 IP 的网络综合起来，如许多业务需要从传感器节点收集数据并传送到因特网中的一个服务器，以开展进一步的分析，或者用户会通过因特网来向 Sink 节点提出请求，需要研究如何让同时运行于两种网络之上的业务获得 QoS 服务的无缝结合。

（5）建立 QoS 度量和服务类型体系。以数据为中心、面向应用的传感器网络以非端到端数据传输为主，需要体现一对多、多对一或多对多的通信模式。因此，结合网络特点和应用需求建立 QoS 度量和服务类型体系是建立和实施 QoS 框架的基础工作[7]。

（6）实时性、可靠性和资源利用率间的自适应 QoS 平衡机制。传感器网络高度冗余的数据可提高数据传输的可靠性，但会消耗过多的能量或存储资源。数据融合可有效减少数据冗余并节省能量，但又会增加传输延迟。通过理论分析或者仿真试验寻找一种最优的自适应 QoS 平衡机制非常重要。

（7）跨优化技术。无线链路在衰落、干扰和噪声等因素作用下信道质量的波动，能量控制策略下节点工作状态的转变，节点增减或移动带来的网络拓扑变化，都需要把物理层的信号质量及时通知 MAC 层，MAC 层也需要及时和网络层、传输层以及应用层进行信息交互。传统分层协议体系体现了“开放”和“互联”，但在面向应用且资源受限的传感器网络中并不是最优的方式。考虑网络各层间的相关性，实施基于跨层优化的 QoS 机制，最

大限度利用有限资源,并在效率、开销、可靠性和可扩展方面求得平衡。

(8)QoS 机制应与节点活动性调度结合。节点活动性调度是节约网络能耗和延长网络生存周期的有效办法。已有研究[3,4,7,8]以数据传输可靠性作为 QoS 度量。因此,选择综合 QoS 度量并结合节点调度和路由机制,为应用提供 QoS 保证值得深入研究。

(9)QoS 控制机制。传感器有时会过度地发送一些数据,有时也会发送一些不充分的数据,既达不到应用的要求,又浪费了宝贵的能源。因此,需要一些集中式或分布式的 QoS 控制机制。

(10)数据传播的 QoS 协议。协议是否具有优先级,当超负荷或在一个高动态的网络中网络能否发送具有高优先级的数据等。

(11)服务。无线传感器网络能提供什么样的非端到端服务,传统的尽最大努力、有保证的、区分的服务能否在新的条件下适用等。

(12)基于聚合性 QoS 参数的 QoS 支持。利用聚合性 QoS 参数为 3 种数据传输模式提供一些支持是很有意义的,需要研究的是这样的机制怎样区分与传统网络的机制。

(13)传统的端到端、能量有效的 QoS 技术。尽管在无线传感器网络中这些不是主要关心的,但在某些情况下它们仍可以适用,而且在某些极端的情况下研究 QoS 的局限性是很有意义的。

(14)折衷。无线传感器网络的数据冗余性可以极大地提高信息的可靠性,然而它消耗极大的能源来传输这些数据。若引入数据融合技术,则可以有效降低数据冗余性,提高能源利用率,但却导致了时延。怎样才能达到最优呢? 只有通过具体的分析或者网络应用,采用折衷的 QoS 才能实现。

13.2　无线传感器网络 QoS 关键技术

针对无线传感器网络在服务质量保障上存在的问题,研究人员已在多个方向上进行着深入探讨。几个主要的关键技术包括能源管理、覆盖机制、数据融合和拥塞控制 4 个方面。

13.2.1　能源管理

能量是传感器网络最受限的资源,因此传感器网络应该关注如何高效利用有限的资源。能源管理不仅能够节省最受限制的资源,而且有助于实现无线传感器网络能量的平衡。传感器网络的能源管理可从低功耗设计、节能软件设计、无线通信、路由协议、网络优化、能量收集等几个方面入手。

在低功耗设计上,可以结合硬件和软件技术节约电能并简化电源设计。例如,选择低功耗的微控制单元(MCU),选用较低的输出电压,尽量使用中断,减少收发模块的启动时间等。

在节能软件设计上,可对操作系统和应用程序接口进行优化。其中,动态电源控制和动态电压调整能使操作系统在性能和能耗控制之间进行折衷;设计良好的应用程序接口 API 应该清晰地注释出能量、质量、时延和操作点等,以便用户建立节能的系统。

在无线通信方面,有 3 种方式来降低能耗。随着传输数据的减少而降低调制等级,降

低传输速度；随着通信距离增加，使用多跳短距离通信以减少单跳通信的距离；减少通信流量。

在路由协议设计方面，必须考虑均匀使用节点能量和数据融合两个方面。从整个网络来看，均匀使用节点能量是为了避免个别节点过早的耗尽，以致缺少某块区域的信息甚至网络瘫痪。而数据融合的作用是减少同一区域内节点数据的冗余性，从而有效降低整个网络的数据流量。

在 MAC 层协议的设计上，首要目的是延长网络系统的生存周期。现阶段对于 MAC 层协议的节能机制研究较为成熟，实现能源控制的措施包括：减少和避免信道访问冲突，利用周期性的监听和睡眠来减少空闲监听时间，避免串音，对大数据进行分段，控制发送功率等。此外，MAC 层协议的可升级性也很重要。

在整个网络的优化上，可从以下两个角度来降低能耗：

(1) 在流量分发方面，可在源和目的地之间寻找一条节能的多跳路由。

(2) 在拓扑管理方面，可降低节点密度，利用较少的节点跟踪事件，从而减小计算的复杂度。

此外，还可通过降低发射功率来减少网络电源的开销。

除了以上策略，能量收集技术的发展也使无电池但具有无限生命周期的无线传感器网络成为可能。能量收集即通过对环境中的机械振动、光能、电磁场、化学能、温度变化、风、热等能量进行收集、转换及存储，并分配到网络传感器的各个部件，从而保证电源需求，实现长期的有效供电。能量收集是无线传感器网络在节能方面的前沿热点技术。现阶段，对于机械振动和光能的能量收集技术已经较为成熟。

13.2.2　覆盖控制

覆盖控制是指在节点能量、网络带宽、计算能力受限的情况下，对传感器节点进行合理放置，并采用适当的路由选择，使无线传感器网络的各种资源得到优化分配。覆盖控制不但提高了能量的有效性，节省网络资源，而且减少了数据的冗余，同时对网络的动态性和可扩展性也有一定的支持。

1. 典型覆盖控制算法与协议

1) 基于网格的覆盖定位传感器配置算法

该算法通过采用网格形式来配置传感器节点以及目标点，传感器节点采用 0/1 覆盖模型，并使用能量矢量来表示格点的覆盖。其目标是在有限的代价条件下，使错误距离最小化，从而优化覆盖识别结果。

2) 轮换活跃/休眠节点的节点自调度覆盖协议

该协议建立在圆形二进制感知模型的基础上，采用节点轮换周期工作机制。在该协议中，每个周期包含一个自调度阶段和一个工作阶段。在自调度阶段里，各节点首先向传感半径内的邻居节点广播通告消息，然后分别判断自身的任务能否由邻居传感器来完成，从而决定进入“休眠状态”还是继续工作，这样便可有效减少网络中的信息冗余。但为了避免出现“盲点”，该协议需要采用一个退避机制以保证网络的充分覆盖。节点自调度覆盖协议不仅对节点冗余进行调度，而且通过节点轮换工作和休眠的机制来减少能源消耗，从而有效延长了网络的生存时间。

3)最佳与最差情况覆盖

该算法考虑的是如何感应并追踪穿越网络的目标或其所在路径上的各点。最佳与最差情况覆盖着重从距离和某些特殊路径的角度来考察网络对目标的覆盖情况。该算法通过设置一定参数来计算无线传感器网络最佳和最差的覆盖情况,并计算出临界的网络路径规划结果。人们可以通过以上结果对网络节点的配置进行指导,从而改进整体网络的覆盖。

4)暴露穿越

暴露覆盖模型更能符合一个实际情况,即目标穿越 WSNs 监视区域的时间越长,被检测到的概率就越大。在该算法中,根据不同的前提条件有不同的确定公式来计算暴露路径,其中最小暴露路径表示无线传感器网络最坏的覆盖情况。

除了以上4种,较经典的覆盖控制算法还有圆周覆盖和连通传感器覆盖等。

2. 覆盖控制有待解决的问题

(1)完善感知模型的种类以适用实际 WSN 环境的多样化需求。

(2)在二维平面研究的基础上解决三维空间覆盖控制的问题。

(3)为具有移动性的网络提供覆盖控制理论。

(4)为在 WSN 和因特网之间交互的数据和信息提供覆盖控制方案。

(5)在研究中引入障碍物的影响。

13.2.3 数据融合

无线传感器网络通过密集分布的大量传感器节点来收集信息。如果原始数据不加处理就直接传送给中心节点,将产生大量的数据冗余,这将给通信网络带来巨大的开销,大大消耗传感器节点的能量,从而减小网络的使用寿命。数据融合,即在每一轮的数据采集过程中,节点采集到的数据包先经过集中汇总,再传输到汇聚节点,这样可以减小数据传输到汇聚节点的次数,减少传感器节点和汇聚节点之间的传输量。可见,数据融合不仅能够减小数据冗余,而且有效节省了网络的能源。下面简单介绍3种典型的数据融合协议。

1. 直接传输法

在该协议中,所有传感器节点都把收集到的数据单独发送给汇聚节点后再进行融合。在直接传输法中,与汇聚节点较远的节点将较快耗尽能量,这容易导致整个网络能量分布很不均匀。此外,在很多情况下,数据产生的地点都具有局部性,因此集中进行数据融合的效率会低于局部信息融合。由此可见,直接传输法适用于传感器节点与汇聚节点比较近,且接收数据消耗的能量比传输数据消耗的能量大很多的网络。

2. 基于层次的 LEACH 协议

在该协议中,监视区域内节点通过自组织的方式构成少量的簇,由每个簇中指定的一个节点对簇内其他节点发送的数据进行收集与融合,并将融合结果发送给汇聚节点。在 LEACH 中,簇头的选择是随机的,因此每个节点都有机会成为簇头,其目的是为了平衡各个节点的能量消耗,从而避免网络能量分布不均的情况。该协议有效延长了网络的生存时间,并提高了数据传输效率。但应该注意到,LEACH 在节约能耗方面还未能做到最佳。

3. PAGASIS 协议

该协议是在 LEACH 协议的基础上改进而来的，被认为是无线传感器网络中接近于理想的数据采集方法。PAGASIS 的基本过程如下：将监视区域内的传感器节点排列成一个链，每个节点都可从最近的邻节点接收并发送数据。当一个节点接收到上一个节点的数据后，先将自己的数据和该数据进行融合，再将数据传送给下一个节点。最后，由一个指定的节点将融合结果传输给汇聚节点。通过 PAGASIS 协议，可以保证每个节点都将数据传输给汇聚节点，且大大降低了节点在每一轮数据传输中耗费的能量。

数据融合技术是无线传感器网络的关键技术之一。根据不同的应用需求以及网络特性，数据冗余情况有很大的差异，因此融合处理方式也有所不同，目前还没有统一的处理模式。

13.2.4　拥塞控制

在无线传感器网络中，不稳定的流量、多对一的通信和多跳的数据传输方式是造成网络拥塞的主要原因。此外，可能造成网络堵塞的还有感知事件之后的突发流量、拓扑结构的高度动态性、频繁变化的无线信道、不同信道上互相干扰的并发数据等。拥塞可能引起丢包率上升、时延增大、能源消耗增多，从而导致全局信道的质量下降。由于网络自身的特点，传统端到端网络的拥塞控制策略不适用于无线传感器网络。

拥塞控制可分为拥塞检测和拥塞减轻两个阶段，这里简单介绍在无线传感器网络研究中现有的几个拥塞控制策略。

1. CoDA(Congestion Detection and Avoidance)

针对基于事件驱动的网络检测到事件引起的拥塞，CoDA 的机制包括基于接收端的拥塞检测，开环 Hop - by - Hop 的后压和闭环多源调节。该算法可调节局部造成的拥塞，并减少逐跳控制信息的能耗，但其中使用的速率调节方式会使距离 Sink 较近的源节点发送更多的分组。

2. ESRT(Event-to-Sink Reliable Transport)

针对 Sink 节点只关心集合信息而不关心单个传感器节点的信息，ESRT 在拥塞监测上采用了基于节点的本地缓冲监测，并根据当前网络的状态进行节点速率的调节。该算法主要适用于 Sink 节点，它可减小网络能耗，提高可靠性，但不适合只发生短暂拥塞、大规模的网络。

3. 自适应的资源控制

该算法针对拥塞期间重要数据包可能丢失的情况，并假设网络中通常有空闲节点可供调度。算法通过创建多元路径对资源供应进行了自适应的调整。该算法采取了拥塞检测、创建选择路径、多路通信 3 个步骤。自适应的资源控制增加了传送分组的精度并节约大量的能量，但多元路径热点距离过近可能引起冲突，而距离初始路径过远还可能增加分组传输延迟和能量消耗。

4. Fusion

该算法结合了 3 种拥塞控制机制，分别是 Hop - by - Hop 流控制、源速率限制模式和有优先级的 MAC 层协议。3 种机制的有机结合减小了信道丢失率，明显改善了网络的有效性和公平性。其弊端是速率限制模式无法杜绝隐终端冲突、歪斜路由、节点故障等

问题。

5. 多到一路由的拥塞控制

针对无线传感器网络多到一的通信导致汇聚节点附件拥塞的问题，该算法通过确定下游子节点最小允许发送速率来减轻拥塞现象。该算法比较简单，可升级，但是对不同深度的节点有较大的影响，同时使用 ACK 也增加了额外开销。

以上是有关无线传感器网络拥塞控制的几种算法。针对不同的拥塞原因以及可能导致的后果，还需要有更多不同的控制策略来解决不同应用上的 QoS 问题。此外，发生拥塞时如何确保应用的 QoS 也是当前的一个研究内容。

13.3　无线传感器网络 QoS 评价指标

无线传感器网络目前还没有统一的参数度量的体系和标准，文献[9]提出适合无线传感器网络的非端到端的概念（Non-End-to-End），即网络所要保证的不是 Sink 与单个传感器节点的端到端之间，而是由应用所决定的 Sink 同“一组”或“多个”处于激活状态进行感知任务的传感器节点之间的 QoS。以图 13.3 中基于事件驱动的应用为例，在工作条件下，定义非端到端的性能参数。即当某事件触发后，监测区域内的一组传感器节点将由休眠状态转变为激活状态，进行感知任务并向 Sink 节点传输采集到的数据。

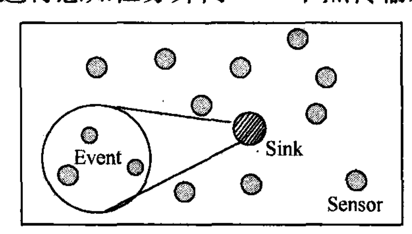


图 13.3　基于事件驱动的无线传感器网络

由此可见，传统的网络 QoS 参数不足以度量无线传感器网络的 QoS 描述需求，需要定义一些新的 QoS 参数，对网络性能进行有效的评价，统称为聚合的 QoS 参数。

【定义 13.1】聚合性时延（Collective Latency）：监测到事件发生后传感器节点产生的第一个数据包与最后一个到达 Sink 的数据包之间的时间差。

【定义 13.2】聚合性丢包率（Collective Packet Loss）：在信息传递过程中与监测事件相关的数据包丢失的数量，而不是单个节点的丢包率。

【定义 13.3】聚合性带宽（Collective Bandwidth）：位于监测区域内的传感器节点向 Sink 节点传输数据所需要的总带宽。

【定义 13.4】信息吞吐量（Information Throughout）：Sink 节点与监测区域内传感器节点之间的总吞吐量。

由上述指标可知，这种非端到端的 QoS 性能指标已不同于传统 IP 网络中端到端的 QoS 度量指标。非端到端的概念所针对的是无线传感器网络面向以数据为中心的应用，把应用所决定的任务交给一组传感器节点来执行，即网络层面的 QoS 问题映射到节点层面来解决。节点层面的 QoS 所要保证的是 Sink 节点与执行任务的多个传感器节点之间的性能指标是否满足 QoS 的要求，而不是针对具体的某个传感器节点。

13.4　无线传感器网络 QoS 路由协议

目前,关于无线传感器网络 QoS 路由协议的研究基本上都是基于传统的端到端的概念,大多并没有考虑到传感器网络中的业务是基于 Event-to-Sink 概念。下面对一些现有 QoS 协议的性能进行比较。

1. 基于传统的端到端概念的 QoS 路由协议

文献[2]提出的有序分配路由(Sequence Allocate Routing,SAR)是为无线传感器网络提出的第一个考虑 QoS 的路由协议,它是一种表驱动多路径(Table Driven Multi - path)的方式,力求获得能量有效性和容错性。该算法在考虑每条路径上的可用能量资源、WS 度量以及每个包的优先权的基础上,以 Sink 节点一跳范围内的邻居节点为根建立生成树,枝干的选择需满足一定 QoS 要求并有一定的能量储备,从而就可以建立起 Sink 到各个节点的多条路径,实际上只使用一条而其他作为备用路径。由于考虑了每个包的优先权,SAR 算法的能耗比最小化能量度量算法更少。多路径可以允许容错和重建,通过加强每条路径中上下行节点间路由表的连贯性来进行失败恢复。但是维护每个节点上的路由表及状态造成了很大的开销,特别是在节点数目众多的情况。

文献[3]中提出一种提供实时端到端软 QoS 保证的路由协议(SPEED)。该协议首先交换节点的传输延迟,以得到网络负载情况,每个节点需要维持其周围邻节点的信息然后利用局部地理信息和传输速率信息作出路由决定,同时通过邻居反馈机制保证网络传输速率在一个全局定义的传输速率阈值之上。节点还通过反向压力路由变更机制避开延迟太大的链路和路由空洞。这样在一定程度上实现了端到端的传输速率保证、网络拥塞控制以及负载平衡机制。但是,SPEED 并没有考虑到任何能量有效性。

文献[10]提出无线传感器网络中另一个考虑 QoS 的路由协议。该协议根据能耗和误码率找到一条开销最小的路径,同时满足特定的端到端延迟需求。另外运用一个基于类的排队模型来同时支持"尽力而为"业务流量和实时业务流量,可以最大化非实时业务的吞吐量。但由于实时业务流量的带宽比率是初始设定且不改变的,这就不能针对不同的链接灵活地调整带宽分配。

虽然上述方法各有优缺点,但它们都是基于传统端到端业务概念的,这可能并不适用于无线传感器网络中的基于 event-to-Sink 概念的业务。

在无线传感器网络中,有多个传感器节点同时采集目标数据,然后再将数据传送给 Sink 以此得到事件的信息,这种独有的业务特点会给 QoS 路由协议设计带来一些独特之处。另外,对资源受限的传感器节点来说,上述协议的机制都太复杂且开销太大。由于新的以数据为中心的路由协议在无线传感器网络中实现的可行性更大,因此应该重点关注怎样在这些协议中实现支持 QoS。

2. 基于可靠性保证的 QoS 路由协议

文献[4]为无线传感器网络提出一种新的可靠的传输方案(ESRT)。它可以在传感器网络中以最小的能量消耗获得可靠的事件探测,更重要的是,这个方案摒弃了传统端到端的概念,考虑了 Event-to-Sink 的概念。该方案包含一个拥塞控制机制,可以同时达到节能和获得可靠性保证的双重目的。其中事件探测的可靠性是由 Sink 节点来控制的,它比

其他传感器拥有更多的能量。但此解决方案仅仅在单独的一个传输层,没有考虑到其他层次比如网络层的一些重要 QoS 因素。

文献[2,3,9]解决了无线传感器网络中一些端到端的可靠性问题,这些方法的新颖之处在于其考虑了信道误差的自适应、信息的重要程度、以及基于数据的重要程度有区分地分配网络资源等问题,这样就使得不同的优先权映射不同的发送可靠性需求。但就像前面所提到的一样,这些可靠性的概念仍然是基于传统的端到端服务的。另外,无线传感器网络的 QoS 概念并不是单纯的一个可靠性问题,其他因素比如等待时间、能量以及带宽问题都应考虑在内。

3. 基于特定业务的 QoS 协议

在文献[5]中,QoS 被定义为在任意给演时间内传送信息的传感器的最佳数量。文章中提出利用基站通过广播信道来向每个传感器传达 QoS 信息,通过 Gur Game 这样一个数学模型来动态调整激活传感器的最佳数量。

文献[3]通过传感器节点调度和数据路由的联合最优化来提供业务的 QoS,相比于没有运用智能调度的方案来说更能延长网络的生命周期。该方案实际上是在业务的可靠性和能量消耗之间找到一个平衡,所以,此文献中的 QoS 仅仅被定义为业务的可靠性。

在其他一些文献(如文献[1,4])中,QoS 还被定义为传感器节点的覆盖范围或是位置排列,其基本思想是怎样覆盖所需要的和有用的区域,不出现感知黑洞,使传感器能够尽可能快和可靠地探测未知事件。传感器节点的布置可以是预先定义好的或是随机的。

13.5 基于跨层设计的 QoS 保障机制

关于无线传感器网络中 QoS 的研究以往基本上是孤立的,或是特定在某些功能层上的研究,或是特别指定某些应用场景的研究。跨层设计是通过层与层之间的信息共享及交换来满足全局的、整体的需要,是对网络进行整体的设计和全局的优化。它模糊了严格的层间界限,将分散在网络各子层的特性参数协调融合,通过信息交互,可以以全局的方式适应特定应用所需的 QoS 和网络实际状况的变化,同时可以根据系统的约束条件和网络特性来进行综合优化,实现对网络资源的有效分配,提高网络的综合性能。可以看出,跨层的设计方法对无线传感器网络来说非常适合。例如,在无线传感器网络的某些应用中,需要网络的生存时间足够长,而时延要尽量短,这对于传感器网络能量有限供应和受限的节点资源和带宽来说是矛盾的,因此,有必要在紧密联系的各功能层之间引入跨层设计的思想。

13.5.1 无线传感器网络基于 QoS 的总体框架

网络体系结构是网络的协议分层,是对网络及其组成部件所应完成功能的定义和描述,而无线传感器网络的网络体系结构是不同于传统网络的,有着其特殊的功能层。文献[15]根据一些研究[8,11]总结出表 13.4 所列的无线传感器网络参考体系结构,然后将无线传感器网络的一系列功能分解到各个功能层上,以便随后在不同层次上进行 QoS 网络性能参数的映射。

可以看出,表 13.4 所列无线传感器网络的网络参考体系结构中,有 1 个水平层(数据管理)和 3 个垂直层(拓扑维护、覆盖维护、节点定位和时钟同步)是明显区别于传统网络的,它们是无线传感器网络的特殊功能层。无线传感器网络网络体系结构中最上面是应用层,无线传感器网络的业务可分为事件驱动型业务、查询驱动型业务、连续型业务和混合型业务。数据管理层提供数据的存储转发、网内处理等功能。从传输层到物理层类似于传统网络的通信协议栈,但运行于高度动态和资源受限的无线传感器网络环境中。传输层提供源传感器节点与接收发送器之间感知数据的传输。网络层将感知数据分组从源传感器节点经选定路由传送至 Sink,同时也采用流量控制来避免拥塞。MAC 层提供传感器节点间在通信范围内的跳到跳的通信,该层还负责包传输的调度和能量节省忙闲周期问题。由于传感器节点工作状态的高度动态性(激活、休眠等)、传感器的随机分布以及部署的高度密集性,需要一个拓扑维护层来维持网络的连通状态,覆盖维护层保证目标区域被最少但足够数量的传感器节点监视。无线传感器网络的用户要把感知数据和实际物理世界中的现象关联起来,所以,节点定位(允许传感器节点对自身定位)和时钟同步(保证传感器节点之间时间的一致性)服务层也是必要的。最底层(基础层,也即物理层)指出了一个传感器节点感知、计算和通信方面的物理能力。

表 13.4 无线传感器网络参考体系结构

<table>
<tr><td colspan="4">应用层
(事件驱动型业务、查询驱动型业务、连续性业务、混合型业务)</td></tr>
<tr><td>数据管理层</td><td rowspan="4">拓扑维护</td><td rowspan="4">覆盖维护</td><td rowspan="4">节点定位
时钟同步</td></tr>
<tr><td>传输层</td></tr>
<tr><td>网络层</td></tr>
<tr><td>MAC 层</td></tr>
<tr><td colspan="4">物理层
(感知能力、处理能力、通信能力)</td></tr>
</table>

1. 应用层

这一层的 QoS 需求一般是由用户来指定的。

2. 数据管理层

数据一般指被网络传输和处理的真实比特,而信息是指已经获得的认知或是从数据中提取出来的结论,这里的数据管理层是指能够理解"信息"的最低层。

3. 传输层

在传统网络中,传输层的任务是为源端机到目的机提供可靠的数据传输,是基于端到端(End-to-End)的概念。而在无线传感器网络的传输层中需要用到"聚合"的概念,只要包含与已接收数据相关的数据分组,都可以看成是一个聚合,属于一个特殊的包。而只有包含与已接收到数据不相关的数据分组才能算另外一个聚合,属于另一个特殊包。

4. 物理层

物理层描述了无线传感器节点各方面的性能,即感知、处理和无线通信这三大组件的性能。感知单元性能包括测量精度、感知范围、感知功率。处理单元性能包括节点定位能力、时钟同步能力、处理速度以及计算能力。无线通信单元性能包括信道速率、编码和射

频功率。一个传感器节点物理的性能会对其他各层的 QoS 需求加以资源的限制:

(1)感知单元。测量精度影响覆盖可靠性、覆盖鲁棒性;感知范围影响覆盖百分率;感知功率影响覆盖维护层的所有 QoS 需求。

(2)处理单元。节点定位能力和时钟同步能力分别影响定位精确度和同步精确度;处理速度决定数据管理层的处理时延;计算能力影响数据管理层的计算花费、数据抽象度和数据精确度,同时也影响节点定位/时钟同步层的服务能量消耗。

13.5.2　无线传感器网络 QoS 需求的权衡关系

受相同低层 QoS 需求影响的两个不同高层 QoS 需求之间的关系,大致有以下 4 种。

1. 竞争关系

两个高层 QoS 需求对低层所提供的有限的资源有着相同的要求。例如,给定数据管理层处理器的处理时延,要改善应用层的响应时间需要更多的 CPU 时间去处理查询信息,而要改善数据更新时间则需要更多的 CPU 时间去处理感知数据,两者将竞争同一有限资源,即 CPU 时间。

2. 对立关系

其中一个高层 QoS 需求的提高需要低层 QoS 需求的提高,而另一个高层 QoS 需求的提高需要同样低层 QoS 需求的降低。例如,提高 MAC 层的通信范围,需要物理层的射频功率更高,而要提高 MAC 层的能量效率,需要射频功率更低。

3. 消长关系

在同一个低层 QoS 需求水平下,改善高层 QoS 需求中的一个会导致另一个 QoS 需求的恶化。例如,在同样的拥塞概率下,提高数据传输的可靠性需要更多冗余数据包的传输,然而这样就增加了能量消耗。

4. 协调关系

两个高层 QoS 需求对低层 QoS 需求的要求是和谐而非对立的,既不竞争同一资源,也不是消长关系。例如,传输层的数据传输可靠性的提高可以使数据管理层的存储丢失率和提取丢失率同时改善,且给定数据传输可靠性后其两者是独立的,所以两者是协调关系。

由此,两个高层 QoS 需求之间只有符合前 3 种关系时才会存在一个权衡点,如在 MAC 层的通信范围和能量效率之间就存在着权衡点,但如果高层 QoS 需求同时受几个低层 QoS 需求的影响,那么就不能采用此种描述方法。另外,还存在一些潜在的权衡点,如果两个 QoS 需求 a、b 之间存在着权衡点,而 A、B 是受这两个 QoS 需求影响的更高层次的 QoS 需求,改善 $a(b)$ 会使得 $A(B)$ 改善或是降低,那么,A、B 之间也会存在一个权衡点,这种规律有助于发现更高层 QoS 需求之间隐藏的权衡关系[15]。

举例说明,连通性维护层的网络直径和网络容量同时都受 MAC 层通信范围的影响,通信范围越大越能改善网络直径,但是通信范围越大,导致邻节点之间的冲突越多,从而使得网络容量下降,所以网络直径和网络容量之间有一个权衡点,而改善网络直径会使得网络层的路径时延改善,改善网络容量会使得网络层的拥塞概率改善,所以,网络层的路径时延和拥塞概率之间也存在着一个权衡点。总之,这些权衡关系的发现能够更加促进理解无线传感器网络系统中跨层之间的相互作用与影响。

13.5.3　基于 QoS 保证的跨层设计

利用表 13.4 提出的无线传感器网络参考体系结构，QoS 可以进行如下跨层设计：

(1) 网络的每一个功能层把会对其他功能层产生影响的 QoS 需求信息直接或间接地传递给相应的层次，如物理层的发射功率、测量精度，MAC 层的通信范围；网络层的拥塞概率等。

(2) 网络的每一个功能层分析从其他功能层传递过来的影响本层性能的 QoS 需求信息，并对本层的通信做出相应的调整。例如，网络层根据拓扑维护层提供的拓扑状况和 MAC 层提供的链路状况实施路由协议，以实现最小路径时延和拥塞概率。

(3) 对于会影响到多个功能层的 QoS 需求参数，要结合业务性能要求对各层进行综合考虑，对相关的性能参数进行折衷考虑。如物理层的射频功率同时影响到 MAC 层的通信范围和传输可靠性、拓扑维护层的网络直径和网络容量、网络层的路径时延和拥塞概率以及传输层的数据传输时延和数据传输可靠性。因此，在进行网络设计时就要充分考虑这些影响，在网络能量消耗、时延、可靠性之间进行有效折衷考虑。

13.6　其他 QoS 保障机制

13.6.1　基于中间件的主动 QoS 机制

主动 QoS 机制建立在应用和网络协商的基础上，可对应用质量、网络结构或路由等进行主动调节与干预。中间件能实现应用与网络间的翻译和控制，支持两者协商新的 QoS。传感器网络的中间件技术的已有研究[19,20]，更多的是集中在中间件问题本身，未上升到 QoS 支持层面。因此，研究如何基于中间件实施主动 QoS 机制值得关注。

如果某些应用提出的 QoS 要求对于网络来说比较难以实施，可以通过应用与网络之间的中间件进行协商，即设计一种中间适配层来适应下层网络和端系统资源的动态变化，它能够方便上下层之间的交互，使上层及时获取得底层的反馈信息并使下层能够准确理解上层数据的语义和贯彻上层的决策，从而提高系统的整体性能和应用感知的服务质量。图 13.4 中，通过在应用与网络之间构建的中间件，可以为无线传感器网络应用屏蔽掉底层平台的差异，应用和网络之间通过中间件的标准 API 接口交换信息，更为重要的是，中间件为主动 QoS 的协商和干预机制，提供了一个收集、分析与判断分散节点信息的合适平台，通过对应用和网络的调整，使当前状态下的网络能够最大限度地支持 QoS 要求，延长网络生命周期。

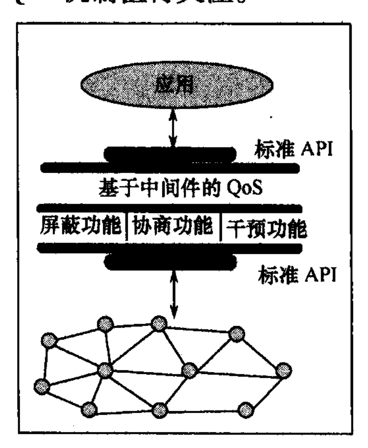


图 13.4　基于中间件的 QoS 技术

13.6.2　QoS 动态资源管理方式

在无线传感器网络中由于动态变化的网络特性，不宜采用静态指配的资源管理方法，

而应采用动态资源管理机制来保证资源分配的高效性。其设计思想是对可允许的资源预留请求规定一个范围，网络在规定的范围内为应用提供服务，采用 QoS 范围而不是单个固定值可以增加 QoS 在请求范围内得到维护的概率，提供软 QoS 保证，并在 QoS_{min} ~ QoS_{max} 之间动态调节应用的 QoS 要求来适应网络资源的变化。动态资源管理的框图如图 13.5 所示，当经过协商后确定资源能够满足 QoS 请求，则可为应用预留和分配所需的资源。否则，需要等待其他流释放资源或重新协商 QoS 要求，并且系统可以根据资源分配和可用资源的变化调节各业务流的速率和占用的资源状况。

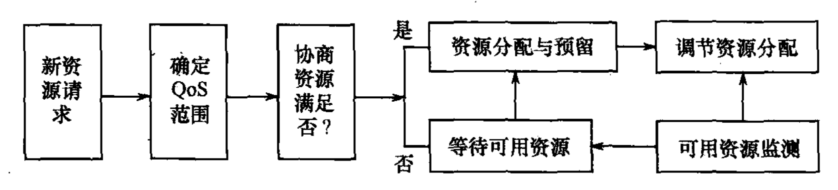


图 13.5　动态资源管理图

动态资源管理和基于中间件的 QoS 技术是提供 QoS 保障非常有效的方法，当网络对应用的支持发生变化后，需要通过动态调节的方式，使网络满足应用对 QoS 的最低要求，或者在降低应用对 QoS 要求的情况下，使网络最大限度地支持应用。这种方法对于网络元素不稳定和整体资源受限的无线传感器网络来说是非常必要的。

13.6.3　确保实时业务的 QoS 方法

无线传感器网络的 QoS 虽然建立在尽力而为、不可靠的数据传输的基础之上，但并不排斥业务流的优先级表达式。当网络中同时具有实时业务和尽力而为的业务时，可以采取以下的方法来确保实时业务对于 QoS 的要求。以图 13.6 为例，在无线传感器网络的一个簇内，簇头节点负责收集来自簇内成员的数据，簇内采用多跳的通信方式，每个负责转发数据的节点对于来自源节点的数据需要进行分类和调度处理，将实时业务和尽力而为业务的数据通过分类器(Classifier)分配到不同队列中，定义带宽比例系数 r 来表示分别用于实时业务和尽力而为业务的带宽比例，根据比例的大小由调度器(Scheduler)来决定不同业务种类分组的传输顺序。建立从源节点到簇头的数据传输路径时，首先要保证能量有效性，计算节点之间的链路代价，主要考虑传输的花费、节点的剩余能量以及信道误码率等因素。

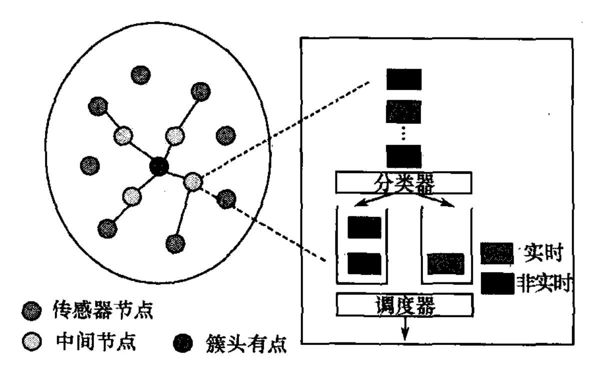


图 13.6　节点的排队与调度模型

13.7　无线传感器网络 QoS 研究面临的挑战

无线传感器网络是一种特殊形式的自组织网络，由于无线传感器网络必须与环境相结合，所以其特征与其他传统数据网络有很多不同。除继承了传统 IP 网络和无线网络中对于 QoS 要求的限制外，本身还具有以下特点：无线传感器网络必须与周围环境相互作用，其特征和传统数据网络有很大的不同。

因此，它除了具有一般无线网络 QoS 支持的大多数问题之外，自身的特征也带来了以下独特的挑战：

(1)严格的资源限制。受限的资源包括能量、带宽、内存、缓冲区大小、处理能力以及传输能力。其中，能量是最主要的，因为它在传感器节点上是最受限制的，且在无人值守或不易到达的区域里为传感器节点更换电池或者给电池充电是不可行的。因此，无线传感器网络中任何的 QoS 机制都必须尽量简单，且要避免使用计算复杂的算法和开销巨大的信令协议。

(2)流量的不对称性。在无线传感器网络的应用中，数据流向是非对称的，通常是多对一的方式，即从大量传感器节点传输到一个 Sink 节点。在设计 QoS 机制时要充分考虑流量的不对称性。

(3)网络的动态性。网络的动态性是由于无线链路的干扰以及节点移动或状态改变等因素造成的，无线传感器网络中存在大量的背景噪声和干扰，信道质量差且带宽有限，节点的链路带宽资源不仅受到邻居节点上业务量变化的影响，还要受到这些节点移动性的影响，这些因素都大大增加了保障 QoS 的难度。

(4)能量平衡。为了实现具有长生命力的网络，必须在所有传感器节点中均匀分布能量载荷，这样可以避免某个或者某个集合(簇内)传感器节点的能量很快被消耗掉。因此，QoS 必须将这个因素考虑在内。

(5)可扩展性。通常无线传感器网络在一个区域内密集分布成百上千的传感器节点。随着节点数或网络密集度的增加，无线传感器网络的 QoS 不能快速地下降，因此应该具有较好的可扩展性。

(6)多个汇聚节点 Sink。一个网络可能存在多个 Sink 节点，它们对网络提出不同的需求。例如，一个 Sink 可能请求位于传感域东北部的传感器节点每分钟发送温度报告，而另一个 Sink 可能只关心西南部异常高温的事件。无线传感器网络应该能够针对不同的 Sink 支持不同的 QoS 等级。

(7)多种业务类型。不同类型传感器的结合将为 QoS 带来挑战，如一些应用程序可能需要不同类型的传感器混合在一起来监测温度、压力以及湿度，因此，需要为这些传感器上设置不同的阅读速率。这种异构环境使 QoS 更具挑战性。

(8)数据包的紧迫性(Packet Criticality)。不同的传感器网络应用具有不同的紧迫性，而应用程序中的数据包也可能具有不同的优先级，因此 QoS 机制可能需要设置不同的数据包紧迫性以及优先级结构[11]。

(9)数据冗余。无线传感器网络的感知数据有着高度的冗余性，虽然数据冗余使得数据传输的可靠性/鲁棒性提高，但却需要花费很多宝贵的能量。数据融合是一个在降低

数据冗余度的同时获得鲁棒性的方法，但此机制也会引起传感器网络中一定的等待时间和复杂的 QoS 设计。

(10)能量和时延之间的平衡。由于无线传输能耗正比于距离的平方或 3 次方(有障碍物遮挡时，μx^k 中的 k 取 2 ~5，一般情况下取 3)，所以无线传感器网络采用了多跳或单跳一多跳相结合的路由，但在能量消耗降低的同时带来了累积增加的数据包时延。另外引入数据融合可以降低数据冗余度来节省能量，但这又给网络带来了更多的延迟，因此有必要找到一个最佳的平衡点。

总而言之，当指定无线传感器网络的一个业务时，以上提出的挑战性问题或多或少要被考虑到。

参考文献

[1] Crawley E, etc. A Framework for QoS-Based Routing in the Internet [EB/OL]. RFC 2386, http://www.ietf.org/rfc/rfc.2386.txt, Aug. 1998.

[2] Sohrabi K, Gao J, Aiiawadhi V, etc. Protocols for Self - Organization of a Wireless Sensor Network[J]. IEEE Personal Communications, pp. 16 - 27, 2000.

[3] He T. SPEED: A Stateless Protocol for Real-time Communication in Sensor Networks[C]. The proceedings of the International Conference on Distributed Computing Systems[A]. Rhode Island, May 2003:46 - 55.

[4] Sankarasubramaniam Y, Nath B, Akyidiz I F. ESRT: Event to Sink Reliable Transport in Wireless Sensor networks[C]. The proceedings of Mobihoc 2003[A], Annapolis, Maryland, June 2003:62 - 70.

[5] Iyer R, Kleinrock L. QOS Control for Sensor Networks[C]. Proceedings of ICC 2003, May 2003, Anchorage, AK, USA, 2003:1340 - 1349.

[6] Meguerdichian S, Koushanfar F, Potkonjak M, etc. Coverage Problems in Wireless Ad-hoc Sensor Networks[C]. Proceedings of IEEE Infocom, 2001, pp. 1380 - 1387.

[7] 史浩山，侯蓉晖，杨少军. 无线传感器网络 QoS 机制研究[J]. 信息与控制，2006.4(35):246 - 250.

[8] SanliH O, Cam H, Cheng X Z. EQoS: an energy efficient QoS protocol forwireless sensor networks[A]. Proceedings of 2004 Western Simulation Multi Conference[C], http://www.easasu.edu/~hasancam/publications/eqos-jan2004.pdf 2004.

[9] 李莉，董树松，温向明. 无线传感器网络中提供 QoS 保障的关键问题[J]. 传感器世界，2006.12:28 - 32.

[10] Akkaya K, Younis M. An energy-aware QoS Routing Protocol for Wireless Sensor Networks[C]. Proc 23rd IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW '03), pp. 710 - 713, Providence, RI, 2003.

[11] Bhatnagar S, Deb B, Nath B. Service Differentiation in Sensor Networks. [C] Proc 4th International Symposium on Wireless Personal Multimedia Communications, 2001.

[12] Deb B, Bhatnagar S, Nath B. ReInForM: Reliable Information Forwarding using Multiple Paths in sensor networks[C]. Proc28th AnnualIEEE Conf on Local Computer Networks(LCN), 2003.

[13] Deb B, Bhatnagar S, Nath B. Information Assurance in Sensor Networks[C]. 2nd International ACM Workshop on Wireless Sensor Network, SanDiego, 2003.

[14] Meguerdichian S, Koushanfar F, Qu G, etc. Exposure in Wireless Ad hoc Sensor Networks[C]. Mobile Computing and Networking, 2001, pp. 130 - 139.

[15] 朱妮，无线传感器网络中 QoS 保证关键技术研究[D]. 南京:南京邮电大学，2006.

[16] Akyildiz I F, etc. A survey on Sensor Networks[J]. IEEE Communication Magazine, 2002: 102 - 114.

[17] Karl H, Willig A. A short survey of wireless sensor networks[R]. TKN, Tech Rep: TKN - 03 - 018, 2003.

[18] 崔莉，李天璞，等．无线传感器网络研究进展[J]．计算机研究与发展，2005：163－135.

[19] Heinzelman W B, Murphy A L, Carvalho H S, etc. Middle-ware to support sensor network applications[J]. IEEE Network, 2004, 18(1): 6－14.

[20] Romer K, Kasten O, Mattern F. Middleware challenges for wireless sensor networks[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2002, 6(4): 59－61.

第14章　无线传感器网络安全技术

网络安全技术历来是网络技术的重要组成部分,没有足够安全保证的网络是没有应用前景的。网络安全问题的涉及面非常广,已不单是技术和管理问题,还有法律、道德方面的问题,需要综合利用数学、管理科学、计算机科学等众多学科的成果予以有效的解决,因此网络安全已经成为一个系统工程。

无线传感器网络作为一种起源于军事领域的新型测控网络技术,其网络安全性问题显得更为重要。由于和传统网络之间存在较大差别,无线传感器网络的安全问题也有一些新的特点。安全涉密保护和网络可靠性问题对无线传感器网络具有十分重要的意义。

无线传感器网络应用系统必须设法取得人们的信任,在许多应用中,网络的安全与保密都是首先需要解决的问题。例如,战场环境中的目标跟踪与监测,自动遥感、遥测,森林火灾、洪水等自然灾害探测与预警,办公环境与健康监测。我国的探月工程,石油运输管道与西气东输工程中温度和压力测量,南水北调的全程监控等均需要保护机制。在诸多的类似应用中,如果传感器信息得不到合理的保护,很可能因此泄露用户和使用信息,甚至泄漏执行的过程信息,其后果往往不堪设想。

无线传感器网络的安全问题包括两个同等重要的方面:网络的实际安全性和用户对网络安全性的感觉。用户对网络安全性的感觉是很重要的,因为用户在通过无线方式传输数据时自然会考虑安全问题,毕竟理论上任何人都可能收到这些数据。通常,用户在采用无线传感器网络应用系统之前用的是有线系统,他们能直观地看到用于信息传输的电线或电缆,因此顺理成章地相信没有其他人在接收他们的信息,也没有人在向他们发送虚假信息。

14.1　无线传感器网络安全概述

无线传感器网络安全与保密性发展的主要动力来自军事应用。军事应用的安全问题最突出,其次是商业应用,保密问题与网络的安全可靠性同样重要。随着无线传感器网络应用的推广和复杂化,保护网络系统正常可靠运行,免受未授权访问的影响变得越来越重要。

无线传感器网络运行于不同的物理环境和不同的约束条件之下。由于无线传感器网络节点资源有限,所以网络需要针对特定应用开发用户定制的原型应用系统结构。由于安全与保密机制需要大量的计算和存储资源,所以,这些机制必须适应相应的传感器系统结构和特定环境中的安全威胁。

随着计算和无线通信能力的增强,传感器节点也从单纯的信息发布扩展到网络处理和分布式计算等更有挑战的任务中。用于网内数据处理的传感器节点和传感器网络的体

系结构容易发生故障,如节点或网络系统能量不足、数据出错率较高等。另外,无线传感器节点的可移动性、动态重配置造成网络结构动态改变,但传感器网络数据采集、数据处理与数据传输必须可靠执行,以确保嵌入式应用结果的正确性和精度。

目前普遍认为,网络安全管理包括以下一些研究内容:

(1)网络实体安全。包括物理条件、物理环境及网络设施的安全标准,嵌入式系统硬件、Sink 硬件、终端及附属设备、网络传输线路的安装及配置等。

(2)网络软件安全。包括保护网络系统不被非法侵入,系统软件与应用软件不被非法复制、修改、不受病毒的侵害等。

(3)网络中的数据安全。包括保护网络信息的数据安全、不被非法存取,保护数据的原始性、完整性、一致性等。

(4)网络安全管理。网络运行时突发事件的安全处理,包括采取计算机安全技术,建立安全管理制度,开展安全审计,进行风险分析等内容。传感器网络安全管理是网络管理中最困难和最薄弱的环节之一。

将有线网络中的入侵检测思想引入到无线传感器网络,是解决无线传感器网络安全问题的一个有效思路,尽管目前在这一领域的研究还处于起步阶段,但是随着越来越多的研究人员参与到这一领域的研究,一定会有更多的安全解决方案呈现出来。

除了安全机制外,维护网络正常、稳定和有效运行的另一个必要措施是网络故障判定及预警机制,可以说,安全机制和故障判定机制是无线传感器网络的一把双刃剑。

14.1.1　网络安全需求

无线传感器网络的安全需求是设计网络安全系统的根本依据。由于无线传感器网络具有和应用密切相关的特点,因此,不同的应用有不同的安全需求,其安全性需求主要源自两个方面:通信安全需求和信息安全需求。

14.1.1.1　通信安全需求

1. 节点的安全保证

传感器节点是构成无线传感器网络的基本单元,节点的安全性包括节点不易被发现和节点不易被篡改。无线传感器网络中普通传感器节点分布密度大,少数节点被破坏不会对网络造成太大影响;但如果入侵者能找到并毁坏各个节点,那么网络就没有任何安全性可言。节点的安全性包括以下两个具体需求:

(1)节点不易被发现。网络中普通传感器节点的数量巨大,少数节点被破坏不会对网络造成太大影响。但是,一定要保证簇头和 Sink 等特殊节点绝对的安全,这些节点在网络中只占极少数,一旦被破坏,则整个网络就面临完全失效的危险。

(2)节点不易被篡改。节点被发现后,入侵者可能从中读出密钥和程序等机密信息,甚至可以重写存储器使该节点"已为它用",因此,要求节点具备抗篡改能力。

2. 被动抵御入侵的能力

无线传感器网络安全系统的基本要求是在网络局部发生入侵的情况下保证网络的整体可用性,但在实际操作中由于诸多因素的制约,实现高性能的网络安全系统是非常困难的。被动防御指的是当网络遭到入侵时网络具备的对抗外部攻击和内部攻击的能力,因此,在遭到入侵时网络的被动防御能力至关重要。被动防御要求网络具备以下能力:

(1)对抗外部攻击者的能力。外部攻击者是指那些没有得到密钥,无法接入网络的节点。外部攻击者无法有效地注入虚假信息,但是可以通过窃听、干扰、分析通信量等活动,为进一步攻击收集信息。因此,对抗外部攻击者首先需要解决保密性问题;其次,要防范能扰乱网络正常运转的简单网络攻击,如重放数据包等,这些攻击会造成网络性能下降;再次,要尽量减少入侵者得到密钥的机会,防止外部攻击者演变成内部攻击者。

(2)对抗内部攻击者的能力。内部攻击者是指那些获得了相关密钥,并以合法身份混入网络的攻击节点。由于无线传感器网络不可能阻止节点被篡改,而且密钥可能被对方破解。因此,总会有入侵者在取得密钥后以合法身份接入网络。由于至少能取得网络中一部分节点的信任,内部攻击者能发动的网络攻击种类更多,危害更大,也更隐蔽。

3. 主动反击入侵的能力

主动反击能力是指网络安全系统能够主动地限制甚至消灭入侵者,为此至少需要具备以下能力:

(1)入侵检测能力。和传统的网络入侵检测相似,首先需要准确识别网络内出现的各种入侵行为并发出警报;其次,入侵检测系统还必须确定入侵节点的身份或者位置,只有这样才能在随后发动有效反击。

(2)隔离入侵者的能力。网络需要具有根据入侵检测信息调度网络正常通信来避开入侵者,同时丢弃任何由入侵者发出的数据包的能力。这样,相当于把入侵者和己方网络从逻辑上隔离开来,可以防止它继续危害网络。

(3)消灭入侵者的能力。要想彻底消除入侵者对网络的危害,就必须消灭入侵节点。但是,让网络自主消灭入侵者是较难实现的。由于无线传感器网络的主要用途是为用户收集信息,因此,可以在网络提供的入侵信息的引导下,由用户通过人工方式消灭入侵者。

14.1.1.2　信息安全需求

信息安全就是要保证网络中传输信息的安全性。对无线传感器网络而言,具体的需求有以下几方面:

(1)数据的机密性:保证网络内传输的信息不被非法窃听。

(2)数据鉴别:保证用户收到的信息来自己方节点而非入侵节点。

(3)数据的完整性:保证数据在传输过程中没有被恶意篡改。

(4)数据的时效性:保证数据在其时效范围内被传输给用户。

综上所述,无线传感器网络安全技术的研究内容包括两方面内容,即通信安全和信息安全。通信安全是信息安全的基础,通信安全保证无线传感器网络内数据采集、融合、传输等基本功能的正常进行,是面向网络基础设施的安全性。信息安全侧重于网络中所传信息的真实件、完整性和保密性,是面向用户应用的安全。

14.1.2　网络安全问题特点

安全问题的一个方面是信息加密的问题。实际上在许多应用系统中,无线传感器网络的重要安全目标并不是加密(保证消息的秘密性或私有性),而是保证接收到的信息没有任何形式的改动并且是所期望的发送者发送过来的。

安全问题的另一个方面是消息验证和完整性校验。一般方法是在发送的消息中添加一个与消息和发送者有关的消息完整性代码(Message Integrity Code,MIC),在安全领域,消息完整性代码通常被称为消息验证码(Message Authentication Code,MAC)①。通信双方共用一个密钥,发送方用其产生 MIC,接收方用其确认消息的完整性和发送者的身份。为了避免窥探者进行"重放攻击",即录下消息并在以后重发给接收方,在计算 MIC 时要包含消息计数器或计时器。这样,不会出现两个经过验证处理的消息是完全相同的,即使是数据也一样。

尽管安全性问题是一个复杂而艰巨的问题,但与传统网络相比,无线传感器网络的特点使其在安全方面有一些独有优势。只有深刻理解无线传感器网络安全问题特点,合理发挥无线传感器网络的安全优势,并据此克服资源受限带来的挑战,才能较好地解决无线传感器网络安全问题。

与传统网络安全问题相比,无线传感器网络安全问题具有以下特点:

(1)内容广泛。传统 Internet 等数据网络为用户提供的是通用的信息传输平台,其安全系统解决的是信息安全传输问题。而无线传感器网络是面向特定应用的信息收集网络,它要求安全系统支持数据采集、处理和传输等更多的网络功能。

(2)需求多样。作为用户和物理环境之间的交互工具,无线传感器网络大多以局域网的形式存在,不论是工作环境还是网络的用途都与传统网络存在很大差距,不同用户对网络性能以及网络安全的需求体现出多样化的特点。

(3)对抗性强。在军事领域中,一些应用使传感器网络本身就是用于进攻或防御的对抗工具。攻击者相关经验丰富、装备先进,并且会动用一切可能的手段摧毁对方网络。对此类无线传感器网络而言,安全性往往是最重要的性能指标之一。

(4)恶劣的应用环境。无线传感器网络可用于战场的恶劣环境中。在这种情形下,节点不能得到有效的保护,可能受到物理攻击,并且对方有可能从受到攻击的节点中获取安全信息。节点抗干扰防护措施的研究是在恶劣环境下保护信息安全的方法。网络的安全机制需要考虑一个或多个节点受到攻击的情况。

(5)资源有限。由于网络节点的尺寸、能量、计算能力和存储空间都受到限制,因此,限制了现有安全算法和协议的使用。无线传感器网络可选的安全解决方案根据资源花费和获得保护之间的合理权衡决定。由于节点获得的资源有限,需要针对新型攻击(如禁止节点休眠)开发相应的防护技术。

(6)网内处理。网络节点通信是能量消耗的主要来源,感知和计算所消耗的能量与之相比少得多。因此,无线传感器网络进行局部处理和数据采集。这种类型的通信为最优安全结构方式,即直接邻域内节点共享一个组合密钥。但在节点易于捕获的环境中,共享对称密钥的机密性容易泄漏。

(7)特定应用结构。无线传感器网络体系必须根据给定的应用条件来设计,牺牲通用结构的灵活性换取资源的有效利用。在特定应用中,网络可以进行适当调整以提高性能并优化资源消耗。这就要求网络设计者确定各种安全攻击的重要性,并据此调整相反的安全机制。

---

① 为了避免与 OSI 协议栈中的 MAC 层使用的缩略语混淆,本文仍使用消息完整性代码(MIC)这个缩略语。

14.1.3 安全问题研究现状

目前,无线传感器网络中的安全问题逐渐成为一个新的研究热点,本小节主要介绍无线传感器网络中的密钥管理、安全路由、安全组播、数据融合和安全定位等方面的研究现状,分析该领域的研究方向。

14.1.3.1 密钥管理

加密和鉴别为网络提供机密性、完整性、认证等基本的安全服务,而密钥管理系统负责产生和维护加密和鉴别过程中所用的密钥。相比其他安全技术,加密技术在传统网络安全领域已经相当成熟,但在资源受限的无线传感器网络中,任何一种加密算法都面临如何在非常有限的内存空间内完成加密运算,同时还要尽量减小能耗和运算时间的同题。在资源严重受限的情况下,基于公开密钥的加密、鉴别算法被认为不适合在无线传感器网络的使用。而无线传感器网络是分布式自组织的,属于无中心控制的网络,因此也不可能采用基于第三方的认证机制。截至目前,密钥管理的研究主要集中在基于对称密钥的加密和鉴别协议上。

1. 单密钥方案

单密钥管理是指无线传感器网络中所有节点共享同一个对称密钥来进行加密和鉴别,它是无线传感器网络中最简单的密钥管理形式。MC Berkeley 的研究人员设计的 TinySec 就使用全局密钥进行加密和鉴别[1]。TinySec 是一个已经在 Mica 系列传感器平台上实现的链路层安全协议,它提供了机密性、完整性保护和简单的接入控制功能。在对节点进行编程时,TinySec 所需的密钥和相关加密、鉴别算法被一并写入节点的存储器,无需在运行期间交换和维护密钥,加之选用了适于在微控制器上运行的 RC5 算法,这使得它具有较好的节能性和实时性。由于 TinySec 在数据链路层实现,对上层应用完全透明,网络的路由协议及更高层的应用都不必关心安全系统的实现,所以其易用性非常好。

加密和解密过程中将消耗大量能量和时间,因此在无线传感器网络中要尽量减少加密、解密操作。为了节省能量和运行时间,研究人员提出 SecureSense 安全框架[2],允许节点根据自己所处的外部环境、自身资源和应用需求为网络提供动态的安全服务,从而减少不必要的加密、解密。SecureSense 也使用开销比较小的 RC5 算法,提供语义安全、机密性、完整性和防止重放攻击等安全机制。

以上两个协议都使用了固定长度的密钥,加密强度是一定的。从理论上说,密钥越长则安全性越好,但是计算开销也越大。为便于根据不同数据包中信息的敏感程度实施不同强度的加密,MCLA 和 Rockwell 开发的 WINS 传感器节点上实现了 Sensor Ware 协议[3],可高效、灵活地利用有限的能量。由于采用了 RC6 算法,无需改变密钥长度,只要简单地调整参数即可改变加密强度,因此非常适合需要动态改变加密强度的场合。

单密钥方案的效率最高,对网络基本功能的支持也最全面;但缺点是一旦密钥泄露,那么整个网络安全服务系统就形同虚设,对无人值守并且大量使用低成本节点的无线传感器网络来说这是非常严重的安全隐患。

2. 多密钥方案

为消除单密钥系统存在的安全隐患可以使用多密钥系统,多密钥管理指的是不同的节点使用不同的密钥,同一节点在不同时刻也可使用不同的密钥。这样的系统相比单密

钥系统要严格得多,即使有个别节点的密钥泄漏出去也不会造成大的危害,系统的安全性大大增强。

SPINS(Security Protocols for Sensor Networks)是一个典型的多密钥协议[4],它提供了两个安全模块,即 SNEP 和 μTESLA。SNEP 通过全局共享密钥提供数据机密性、双向数据鉴别、数据完整性和时效性等安全保障。μTESLA 首先通过单向函数生成一个密钥链,广播节点在不同的时隙从中选择不同的密钥计算报文鉴别码,再延迟一段时间公布该鉴别密钥。接收节点使用和广播节点相同的单向函数,它只要和广播者实现时间同步就能连续鉴别广播包。由于 μTESLA 算法只认定基站是可信的,只适用于从基站到普通节点的广播数据包鉴别,普通节点之间的广播数据包鉴别必须通过基站中转。因此,多跳网络中有大量节点卷入鉴别密钥和报文鉴别码的中继过程,除了可能引发安全方面的问题,由此带来的大量通信开销也是以广播通信为主的无线传感器网络难以承受的。

LEAP 协议采用了另一种多密钥方式:每个节点和基站之间共享一个单独的密钥,用于保护该节点发送给基站的数据。网络内所有节点共享一个组密钥,用于保护全局性的广播。为保障局部数据聚合的安全进行,每个节点都和它所有的邻节点之间还共享一个簇密钥。同时任意节点都与其每个邻节点之间拥有一个单独的会话密钥,用于保护和邻节点之间的单播通信,由于 LEAP 协议使用不同的密钥保护不同的关系,其对上层网络应用的支持好于 SPINS 协议,但其缺点是每个节点要维护的密钥个数比较多,开销较大。

为降低密钥管理系统传输密钥带来的风险,减小用于密钥管理的通信量,可采用随机密钥分配机制。通过从同一个密钥池中随机选择一定数量的密钥分配给各个节点,就能以一定的概率保证其中任意一对节点拥有相同的密钥来支持相互通信. 随机分配机制不必传输密钥,能适应网络拓扑的动态变化,安全性较好,但是其扩展性仍然有限,难以适应大规模的网络应用。

由于入侵者很难同时攻破所有密钥,多密钥的安全性较好,但是采用多密钥管理方案时,网络中必须有部分节点承担繁重的密钥管理工作,这种集中式的管理不适合无线传感器网络分布式的结构。这种结构性差异引起一系列问题,当网络规模增大时,用于密钥管理的能耗将急剧增加,影响系统的实际可用性。此外,多密钥系统仍无法彻底解决泄露问题。

14.1.3.2　安全路由

无线传感器网络中一般不存在专职的路由器,每一个节点都可能承担路由器的功能,由于对于任何路由协议,路由失败都将导致网络的数据传输能力下降,严重的会造成网络瘫痪,因此路由必须是安全的。但现有的路由算法如 SPIN、DD、LEACH 等都没有考虑安全因素,即使在简单的路由攻击下也难以正常运行。

与外部攻击者相比,那些能够发送虚假路由信息或者有选择地丢弃某些数据包的攻击者对路由安全造成的危害最大,因此,网络安全系统要具有防范和消除这些内部攻击者的能力。当前,实现安全路由的基本手段有两类:一类是利用密钥系统建立起来的安全通信环境来交换路由信息;另一类是利用冗余路由传递数据包。

实现安全路由的核心问题在于拒绝内部攻击者的路由欺骗。因此有研究者将 SPIN 协议用于建立无线自组网络的安全路由,这种方法也可以用于无线传感器网络。在这类方法中,路由的安全性取决于密钥系统的安全性。无线传感器网络的密钥系统是脆弱的,

难以抵消设计巧妙的网络攻击。例如，在虫洞（Wormhole）攻击中，完全是基于入侵者拥有的强大硬件设施发动的，根本就不靠窃取密钥等方法接入网络；密钥系统对此类网络攻击无能为力。

J. Deng等研究人员提出了对网络入侵具有抵抗力的路由协议INSENS。在这个路由协议中，针对可能出现的内部攻击者。网络不是通过入侵检测系统，而是综合利用了冗余路由及认证机制化解入侵危害。虽然通过多条相互独立的路由传输数据包可能避开入侵节点，但使用冗余路由也存在相当大的局限性，因为冗余路由的有效性是以假设网络中只存在少量入侵节点为前提的，并且仅仅能解决选择性转发和篡改数据等问题。而无法解决虚假路由信息问题冗余路由在实际网络使用中也存在问题，如在网络中难以找到完全独立的冗余路径，或者即使成功地通过多条路由将数据传递回去，也将导致过多的能量开销。

14.1.3.3　安全组播[5,6]

由于无线传感器网络的一个重要应用是军事，因此，为了防止对方向网络注入伪造的信息或者错误的管理信息，需要在无线传感器网络中实现基于源端认证的安全组播。但是在无线传感器网络中，不推荐使用公钥密码体制或耗费资源的其他机制，因此，源端认证的组播并不容易实现。目前，在无线传感器网络中普遍采用的组播协议是μTELSA，该协议是Perrig等人针对无线传感器网络的特点在μTELSA协议的基础上提出的鉴于时间的数据丢包的流认证协议①。μTELSA的主要思想是先广播一个通过密钥K认证的数据包，然后公布密钥K。那么，在密钥K公布之前，没有人能够得到密钥的任何信息，也就没有办法在广播包认证之前伪造正确的广播数据包。

在μTELSA协议中，节点使用SNEP协议加入网络的过程是一个点对点的单播过程，这样的操作在大规模传感器网络中需要消耗大量网络资源。此外，单一的密钥链导致基站保存过长的密钥链或者同步时间间隔过长，或者需要多次重构密钥链。

针对以上问题有人提出了多级μTESLA协议，多级μTESLA协议预先配置初始化密钥并由基站广播同步时钟参数，避免了使用SNFP协议建立点对点安全通信。相比μTESLA协议，多级μTESLA协议具有比较好的网络特性。但其实现的复杂度比较高，并且占用了更多的节点内存和计算资源。此外，μTELSA和多级μTELSA都不可避免地具有认证延迟的特点，使得攻击者能够利用这一缺陷破坏μTELSA初始参数的分发过程。

μTELSA协议中，多级μTELSA协议之后又有人提出了PBA（Practical Broadcast Authentication）协议。方案便用Merkle哈希树认证和发布多个发送者的μTELSA参数，从而避免了μTELSA原有的认证延迟的特点。另外，对被俘获的节点，该方案通过生成撤销树来抵御俘获攻击。然而，对撤销树的维护会引起较大的系统开销，并且此方案不支持新的发送者的加入。

14.1.3.4　安全数据聚合

数据聚合是无线传感器网络的主要特点之一，在无线传感器网络中，大量的传感器节点被部署在指定区域。对于一个数据查询请求，如果从多个节点返回大量的未经过处理

① TESLA认证广播是一种比较高效的认证广播协议，最初是为组播认证设计的。

的数据，则有悖于传感器网络本身非常受限的网络资源的特性。因此，数据在传输的过程中被融合节点聚集和处理，通过在网络内聚合多个节点采集到的原始数据，可以达到减少通信次数、降低通信能耗，从而延长网络生存时间的作用。目前，在无线传感器网络内实现安全数据聚合主要通过以下两个途径：

(1) 提高原始数据的安全性。就是要保证用于聚合的原始数据的真实性。现有的手段主要是数据认证，但现有的高强度认证机制不但引入了更多的时间和能量开销，还限制了网络的数据聚合能力，而那些对数据聚合支持较好的协议又存在比较严重的安全隐患。

(2) 使用安全数据聚合算法。由于相邻节点采样值具有相似性，聚合节点可通过对多个原始数据进行综合处理来减轻个别恶意数据的危害。但这种办法也存在局限性，聚合节点并不总能获得多个有效的冗余数据，而且对于不同的应用效果也不同。在环境监测等时间驱动型应用中可能取得较好效果，但是在目标侦查、定位等事件触发型应用中，这样做不但会引起更大的延时，还可能把重要信息过滤掉。

14.1.3.5　安全定位

传感器节点必须明确自身位置才能详细说明在“什么位置或区域发生了特定事件”，才能实现对外部目标的定位和追踪。对于大多数应用不知道传感器位置而感知的数据是没有意义的。无线传感器网络中的定位方法基本上都采用几何的方法，利用已知位置的节点作参照计算出未知节点的位置，但如何在开放、敌对的环境下安全地定位节点仍是一个值得研究的课题。

节点的安全定位包括两个方面的内容：一是节点如何安全地确认或者计算自己的位置信息；二是节点如何安全地确认其他节点的位置信息。

14.1.4　安全问题研究的挑战

尽管无线传感器网络安全技术的研究取得了很大进展，在复杂的安全环境、多样的安全需求和无线传感器网络自身资源限制等因素的综合作用下，还有一些问题尚未完全解决，其安全性技术仍然面临以下一些挑战：

(1) 无线传感器网络中节点自身资源严重受限，能量有限，处理器计算能力弱，通信带宽小，内存容量小，这极大地限制了传感器节点本身的对抗能力。

(2) 无线传感器网络主要采用无线通信方式，与有线网络相比，其数据包更容易被截获，其信道的质量较差，可靠性比较低，也更容易受到干扰。

(3) 无线传感器网络内不存在控制中心来集中管理整个网络的安全问题，所以，安全系统必须适应网络的分布式结构，并自行组织对抗网络入侵。

关于安全性，无线传感器网络设计还面临以下 3 个问题：

(1) “MIC 的长度及安全计划”必须与所传输数据的典型长度相平衡，必须考虑减少发送消息的长度要求。尽管对于安全性要求较高的系统，一般需要采用 14B 的 MIC，而当只需传输一位数据信息时，14B 的 MIC 就显得很笨拙了。开发人员必须在“网络低功耗需求”与“用户安全要求”之间求得平衡。因此，需要选择合适的 MIC 长度，并综合考虑消息验证、完整性校验和加密问题。此外，为了满足网络自组织的需要，所有这些安全管理功能必须能自动地执行。

(2)安全功能的实现必须采用廉价的硬件,包括使用尽可能少的逻辑门电路、随机访问存储器和只读存储器,以降低网络设备的成本。由于大多数网络设备的计算能力是很有限的,上述门电路使用少、内存占用少、执行指令数量少等各种设计要求限制了可使用的安全算法种类。

(3)最难解决的问题或许还是密钥分发问题。密钥分发方法有很多种,如有些方法采用专门的密钥加载设备,有些方法需要用户进行某种形式的直接参与等。在具体的应用系统中,它们各有优缺点,无线传感器网络开发人员必须为手头的应用系统选择最合适的方法。

在面临这些挑战性问题的同时,与传统网络相比,无线传感器网络在安全方面也具有自己独有的优势。

(1)无线传感器网络是典型的分布式网络,具备自组网能力,能适应网络拓扑的动态变化,再加上网络中节点数目众多,网络本身有较强的可靠性,所以无线传感器网络对抗网络攻击的能力较强,遇到攻击时,一般不容易出现整个网络完全失效的情况。

(2)随着 MEMS 技术的发展,完全可能实现传感器节点的微型化。在那些对安全要求高的应用中,可以采用体积更小的传感器节点和隐蔽性更好的通信技术,使网络难以被潜在的网络入侵者发现。

(3)无线传感器网络是一种智能系统,有能力直接发现入侵者。有时网络入侵者本身就是网络要捕捉的目标,在发起攻击前就已经被网络发现,或者网络攻击行为也可能暴露攻击者的存在,从而招致网络的反击。

(4)无线传感器网络不具有其传统网络的通用性,每个网络都是面向特定应用设计的。目前没有统一的标准,在这种情况下入侵者无法形成通用的攻击手段。

解决无线传感器网络安全问题的最终目标是以最小的开销获得尽可能多的安全保证,要达此目标,存在以下途径:

(1)获得实际对抗网络入侵的经验。已有的研究工作都是基于各种“假设”进行的,还无法了解无线传感器网络入侵的实际工作方式和后果。通过实际对抗可以检验这些假设的合理性,评判已有研究工作的有效性,发现对无线传感器网络安全问题的认识误区,这些都有助于改进和深化现有的研究工作,更重要的是可能会由此发现解决问题的新方向或更有效的方法。

(2)拓展现有研究的深度和广度。目前,能用于解决无线传感器网络安全问题的基本手段非常有限,主要的几种安全技术,如安全路由、安全聚合和入侵检测等都是刚刚开始探索,在无线传感器网络中实现这些技术现在还存在很多困难。但是从长远看,它们可能会在安全系统中发挥重要作用,因此对这些基本技术还需要作进一步研究。未来随着无线传感器网络的大量推广应用,与因特网的互联会越来越多,诸如防火墙、防病毒等技术也会成为无线传感器网络安全问题的研究内容。

(3)探索高效的安全系统集成方法。就传统经验而言,网络安全仅靠一两种技术是不可能解决无线传感器网络安全问题的。即便将来各个单项安全技术都取得进展,仍将面临系统集成问题。由于无线传感器网络具有面向应用的特点,与因特网相比,要在一个实际网络中综合应用这些技术会面临更多的困难。因此,根据不同网络的实际需要优化配置各项安全技术将是实现上述最终目标的关键一步。

14.2 安全问题策略分析

无线传感器网络的安全隐患在于网络部署区域的开放特性和无线电通信的广播特性,网络部署区域的开放特性是指无线传感器网络通常都部署在应用者无法直接进入的区域内,所以存在受到无关人员或者敌方人员破坏的可能性。无线电通信的广播特性是指通信信号在物理空间上是暴露的,任何设备,只要调制方式、频率、振幅和相位与发送信号匹配,就能够获得完整的通信信号。这种广播特性使无线传感器网络的部署非常高效,只要保证一定部署的密度,就能很容易地实现网络的连通特性;但同时也带来了信息泄漏和空间攻击等安全隐患。

无线传感器网络协议栈由物理层、数据链路层、网络层、数据融合层、传输层和应用层组成,安全问题在网络协议的各个层次都应该充分考虑,但是研究的侧重点不尽相同。物理层机密性考虑主要侧重在安全编码方面;链路层和网络层机密性考虑的是数据帧和路由信息的加解密技术;而应用层在机密性方面的研究则是密钥的管理和交换过程,为下层的加解密技术提供安全支撑。

14.2.1 物理层安全问题

物理层面临的主要安全问题是无线通信的干扰和节点的破坏,遭受的主要攻击包括拥塞攻击和物理破坏。

1. 拥塞攻击

无线环境是一个开放的环境,所有无线设备共享这样一个开放的空间。如果两个节点发射的信号在一个频段上,或者频点很接近,则会因为彼此干扰而不能正常通信。拥塞攻击只要获得或者检测到网络通信频率的中心频率,就可以通过在这个频点附近发射无线电波进行干扰,因此,拥塞攻击对单频点无线通信网络非常有效。

要抵御单频点的拥塞攻击,使用宽频和调频的方法是比较有效的。在检测到所在空间频率遭受攻击以后,网络节点将通过统一的策略跳转到另外一个频率进行通信。对于全频长期持续拥塞攻击,转换通信模式是唯一能够使用的方法(光通信和红外线等无线通信方式也都是有效备选方法)。由于全频持续拥塞攻击在实施时存在很多困难,攻击者一般不采用全频段持续攻击,因此,无线传感器网络可以采取一些更加积极有效的办法应对拥塞攻击。例如,当攻击者使用能量有限持续的拥塞攻击时,节点采取不断降低自身工作占空比的方法,可有效对付这种攻击。当攻击者为了节省能量,采用间歇式拥塞攻击方法时,节点可以利用攻击间歇进行数据转发。如果攻击者采用的是局部攻击,节点可以在间歇期间使用高优先级的数据包通知基站遭受拥塞攻击的事实。

2. 物理破坏

因为无线传感器网络节点往往分布在较大的区域内,所以保证每个节点的物理安全是不可能的,敌方人员很可能俘获一些节点,对其进行物理上的分析和修改,并利用它干扰网络正常功能。针对无法避免的物理破坏,需要无线传感器网络采用更精细的控制保护机制。

(1)完善物理损害感知机制。节点能够根据其收发数据包的情况、外部环境的变化

和一些敏感信号的变化，判断是否遭受物理侵犯。一旦感知到物理侵犯就可以采用具体的应对策略，使敌人不能正确分析系统的安全机制，从而保护网络剩余部分免受安全威胁。

（2）信息加密。现代安全技术依靠密钥来保护和确认信息，而不是依靠安全算法，所以，通信加密密钥、认证密钥和各种安全启动密钥需要严密的保护。由于传感器节点的限制，其有限计算能力和存储空间使基于公钥的密码体制难以应用于无线传感器网络中，为了节省传感器网络的能量开销和提供整体性能，也要尽量采用轻量级的对称加密算法。

Prasantb Gonesan 等人详细分析了对称加密算法在无线传感器网络中的负载，他们在 Atmega103、Atmega 108、M14C/10 等 5 种嵌入式平台构架上分别测试了 RC4、RC5、IDEA、SHA1 和 MD5 这 5 种常用的对称加密算法的计算开销。测试表明，在无线传感器平台性能最优的对称加密算法是 RC4，而不是目前传感器网络中所使用的 RC5。由于对称加密算法的局限性，不能方便地进行数字签名和身份认证，这给无线传感器网络安全机制的设计带来了极大的困难，因此，高效的公钥算法是无线传感器网络安全需要解决的问题。

14.2.2　链路层安全问题

1. 碰撞攻击

碰撞指的是当两个节点同时发送数据时，它们的输出信号会因信道冲突而相互叠加，从而导致数据包的损坏，发生在链路层协议中的信道冲突称为碰撞。针对碰撞攻击，目前主要有以下两种处理方法：

（1）使用纠错编码。纠错码是为了解决低质量信道的数据通信问题，通过在通信数据包中增加冗余信息来纠正数据包中的错误位。纠错码的纠正位数和算法的复杂度与数据信息的冗余度相关，通常使用 1 位 ~2 位纠错码。如果碰撞攻击者采用的是瞬间攻击，只影响个别数据位，那么使用纠错编码是有效的。

（2）使用信道监听和重传机制。节点在发送前先对信道进行一段随机时间的监听，在预测信道一段时间为空闲的时候，开始发送降低碰撞的概率。对于有确认的数据传输协议，如果对方表示没有收到正确的数据包，则需要将数据重新发送。

2. 耗尽攻击

耗尽攻击就是利用协议漏洞，通过持续通信的方式便节点能量资源耗尽，应对耗尽攻击的一种方法是限制网络发送速度，节点自动抛弃那些多余的数据请求，但是这样会降低网络效率；另外一种方法就是在协议实现的时候，制定执行策略，对过度频繁的请求不予理睬，或者对同一个数据包的重传次数进行限制，以避免恶意节点无休止干扰导致节点能源耗尽。

3. 非公平竞争

如果网络数据包在通信机制中存在优先级控制，恶意节点或者被俘节点可能会不断在网络上发送高优先级的数据包占据信道，从而导致其他节点在通信过程中处于劣势。这是一种弱 DoS 攻击方式，需要敌方完全了解传感器网络的 MAC 层协议机制，并利用 MAC 的协议来进行干扰性攻击。一种解决的办法是采用短包策略，即在 MAC 层中只使用较短的数据包，这样就可以缩短每包占用信道的时间；另外一种解决办法就是弱化优先级之间的差异或者不采用优先级策略，而采用竞争或者时分复用方式实现数据传输。

14.2.3　网络层与数据融合层安全问题

由于每个传感器节点与簇头节点都是潜在的路由节点，因此更易于受到攻击。网络层的主要攻击有以下几种：

(1)虚假的路由信息。通过欺骗、更改和重发路由信息，攻击者可以创建路由环，吸引或者拒绝网络信息流通量，延长或者缩短路由路径，形成虚拟的错误消息、分割网络、增加端到端的时延等。

(2)选择性的转发(Selective Forwarding)。节点收到数据包后有选择地转发或者根本不转发收到的数据包，导致数据包不能到达目的地。

(3)Sinkhole 攻击。攻击者通过声称自己电源充足、可靠而且高效等手段，吸引周围的节点选择它作为其路由路径中的点，然后和其他的攻击(如选择攻击，更改数据包的内容等)结合起来，达到攻击的目的。由于传感器网络固有的通信模式，即通常所有的数据包都发到同一个目的地，因此特别容易受到这种攻击的影响。

(4)Sybil 攻击。在这种攻击中，单个节点以多个身份出现在网络中的其他节点面前，使其更易于成为路由路径中的节点，然后和其他攻击方法结合使用，达到攻击的目的。

(5)Wormhole 攻击。如图 14.1 所示，这种攻击通常需要两个恶意节点相互串通，合谋进行攻击。一般情况下，一个恶意节点位于簇头节点附近，另一个恶意节点离簇头节点较远。较远的那个节点声称自己和簇头节点附近的节点可以建立低时延和高带宽的链路，从而吸引周围节点将其数据包发到它这里。在这种情况下，远离簇头节点的那个恶意节点其实也是一个 Sinkhole。Wormhole 攻击可以和其他攻击(如选择转发、Sybil 攻击等)结合使用。这一点也体现在数据融合层当中。

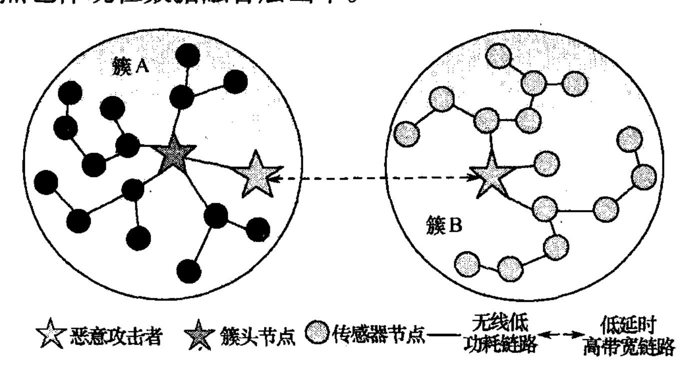


图 14.1　Wormhole 攻击

(6)HELLO flood 攻击。很多路由协议需要传感器节点定时发送 HELLO 包，以声明自己是它们的邻节点，但是一个较强的恶意节点以足够大的功率广播 HELLO 包时，收到 HELLO 包的节点会认为这个恶意节点是它们的邻居。在此后的路由中，这些节点很可能会使用这条由恶意节点建立的路径，向恶意节点发送数据包。如果网络节点离恶意节点距离较远，以普通发射功率传输的数据包根本到不了目的地，从而造成节点增大发射功率及延长工作时间，使节点过早的因能量耗尽而退出网络。

(7)确认欺骗。一些传感器网络路由算法依赖于潜在的或者明确的链路层确认。由于广播媒介的内在性质，攻击者能够通过偷听通向邻近节点的数据包，发送伪造的链路层

确认。目标包括使发送者相信一个弱链路是健壮的，或者是相信一个已经失效的节点还可以使用。由于沿着弱连接或者失效连接发送的数据包会发生丢失，攻击者能够通过引导目标节点利用那些链路传输数据包，从而有效地使用确认欺骗进行选择性转发攻击。

以上攻击类型有可能被单独使用，也可能组合使用，其攻击手段通常是以恶意节点的身份充当网络中的成员节点，被网络误当作正常的路由节点来使用。恶意节点在冒充数据转发节点的过程中，可随机丢掉其中的一些数据包，或者通过修改源地址和目的地址，选择一条错误路径发送出去，从而破坏网络的通信秩序，导致网络的路由混乱。解决的办法之一就是使用多路径路由这样即使恶意节点丢弃数据包，数据包仍然可以从其他路径送到目标节点。

对于分簇型层次式路由机制，可以使用输出过滤（Egress Filtering）方法①。这种方法通过认证源路由的方式确认一个数据包是否是从它的合法簇头发送过来的，直接丢弃不能认证的数据包。这样，攻击数据包在前几级的节点转发过程中就会被丢弃，从而达到保护目标节点的目的。

数据融合层的攻击主要是恶意节点充当簇头节点或 Sink 节点，将恶意信息参与数据融合，并通过 Sink 节点传输到网外，如进入因特网或以太网等。

14.2.4　传输层与应用层安全问题

传输层用于建立无线传感器网络与因特网或其他外部网络的端到端的连接。由于无线传感器网络节点的限制，节点无法保存维持端到端连接的大量信息，而且节点发送应答消息会消耗大量能量，因此，目前关于无线传感器节点传输层协议的安全性研究还很少。Sink 节点是无线传感器网络与外部网络的接口，传输层协议一般采用传统网络协议，但需要实现嵌入式构建，通过精简和优化以适合于 Sink 节点。此外，还需要解决 Sink 节点的数据传输瓶颈等问题。

应用层提供无线传感器网络的各种实际应用。应用层的密钥管理和安全组播为整个无线传感器网络的安全机制提供了安全基础设施，因此，应用层的安全研究主要集中在为整个无线传感器网络提供安全支持的研究，也就是密钥管理和安全组播的研究。

14.3　无线传感器网络认证机制

认证技术是无线传感器网络安全中的重要问题，认证主要包括实体认证和信息认证。实体认证是接入控制的中心问题②，用于鉴别用户身份。而信息认证则主要是确认信息源的合法身份以及保证信息的完整性，防止非法节点发送、伪造和篡改信息。

14.3.1　信息安全威胁与认证目标

从用户角度来看，恶意用户常采用以下手段对网络系统进行攻击：

---

① 输出过滤（egress filtering）方法：用于在因特网上抵制方向误导攻击。

② 实体认证：根据著名密码学专家 Meneges 的定义，它是在网络中一方根据某种协议确认另一方身份的过程，给网络的接入提供安全准入机制，是无线传感器网络安全的第 1 道屏障。

(1)窃取口令。非法用户获得合法用户身份的口令,这样非法用户就获得授权,可以访问系统资源。

(2)流量分析。非法用户对通信双方交换的信急进行分析,试图判断或还原“源信息”。

(3)重传。非法用户截获信息,然后再传送给接收者。

(4)修改或伪造。非法用户截获信息,替换或修改信息后再传送给接收者,或非法用户冒充合法用户发送消息。

(5)阻断服务。阻止系统资源的合法管理和使用。

因此,网络安全服务应当提供如下认证的功能:

(1)可信性。信息的来源是可信的,信息接收者能够确认所获得的信息不是由恶意节点所发出的。

(2)完整性。要求信息在传输过程中保证其完整性,信息接收者能够确认所获得的信息在传输过程中没有被修改、延迟和替换。

(3)不可抵赖性。要求信息的发送方不能否认用户所发出的信息。同样,信息的接收方不能否认已收到了信息。

(4)访问控制。非法用户不能够访问系统资源,合法用户只能访问系统授权和指定的资源。

14.3.2　基本认证协议

认证所采用的技术主要有两类:公钥加密算法(如数字签名)和对称加密算法(如消息识别码 MAC)。

1. 非对称认证协议

这类协议采用公钥加密算法,在该类协议中每个实体都有认证中心(CA)颁发的证书 <PK> 和指定的公私密钥对。其公钥信息认证过程的算法如下:

(1)A 用自己的私钥给信息 m 签名为 $S = \mathrm{SIG}(m, SK)$ 并发送 m, S, <PK> 给 B。

(2)B 首先验证证书 <PK> 的合法性并获得 A 的 PK,然后再用该 PK 验证 S 的合法性。

该算法如再引入随机数 r(这里,随机数 r 用来抗重播)和请求—应答机制(ACK)则可转化为公钥实体认证协议,算法如下:

(1)B 发送一个随机数给 A。

(2)A 发送 $\mathrm{SIG}(r, \mathrm{PK})$, <PK> 给 B。

(3)B 验证证书 <PK> 的合法性,然后再用获得的 A 的公钥验证签名 $\mathrm{SIG}(r, \mathrm{PK})$。

2. 对称认证协议

这类协议采用对称加密算法。在这类协议中有一可信 Sink 节点 S 来建立起 A 和 B 的信任关系,每个实体都和该 Sink 节点共享一个对称密钥。首先 A 向 S 发起一个请求信息,请求和 B 建立信任关系,然后 S 就给 A 和 B 发送一个认证会话密钥 K。

该信息认证过程算法如下,其中 $E(m, K)$ 表示由密钥 K 加密的信息 m, $\mathrm{MAC}(m, K)$ 表示 m 和 K 形成的消息识别码,K 表示 Sink 节点 S 和 A 共享的秘密密钥。算法如下:

(1)A 发送一请求信息给 S。

(2) S 发送 $E(m, K)$ 给 A，同时发送 $E(K, Kp)$ 给 B。

(3) A 计算消息识别码 $M = \mathrm{MAC}(m, K)$，并发送 m、M 给 B。

(4) B 验证 M。

同样，它也可以通过引入随机数而转化为实体认证协议：

(1) A 发送一请求信息给 S。

(2) S 发送 $E(K, K_a)$ 给 A，同时发送 $E(K, K_b)$ 给 B。

(3) B 发送随机数 r 给 A。

(4) A 计算消息识别码 $M = \mathrm{MAC}(r, K)$ 并发送 M 给 B。

(5) B 验证 M。

在该类协议中，如每个节点都预置了相互的对称密钥，则 Sink 节点的操作可以去掉，使得对称 MAC 信息认证只需进行步骤(3)和步骤(4)，对称 MAC 实体认证只需进行步骤(3) ~ 步骤(5)。

3. 混合型认证协议

该类认证协议采用的是密钥协商协议（如 Diffie-Hellman）和对称 MAC 协议合并使用的办法来达到采用公钥算法同样的效果。算法一和算法二表示这种混合协议的过程，其中，a 和 b 作为私钥是各自保密的。$K_A = a \cdot G$，$K_B = b \cdot G$，作为 A 和 B 的公钥以及基数 G 可以是公开的。

【算法 14.1】混合信息认证

(1) A 发送其公钥 K_A 给 B，B 也发送其公钥 K_B 给 A。

(2) A 计算出对称密钥 $K = a * K_A$，B 也计算出同一对称密钥 $K = b * K_B$。

(3) A 计算消息识别码 $M = \mathrm{MAC}(m, K)$ 并发送 m，M 给 B。

(4) B 验证 M。

【算法 14.2】混合实体认证

(1) A 发送其公钥 K_A 给 B，B 也发送其公钥 K_B 给 A。

(2) A 计算出对称密钥 $K = a * K_A$，B 也计算出同一对称密钥 $K = b * K_B$。

(3) B 选择一随机数 r 发送给 A。

(4) A 计算消息识别码 $M = \mathrm{MAC}(r, K)$ 并发送 M 给 B。

(5) B 验证 M。

4. 时间标记认证协议

通过证明时间标记的有效性也可以做到实体认证，这和采用随机数的办法效果一样。这里加入了接收方的身份标示符作为认证信息来抗重播，当前时间 t 作为时间标记，算法如下：

(1) A 计算 $M = E(t|B, K)$，并发送 M 给 B；

(2) B 验证时间标记 t 和身份表示符是否有效。

14.3.3　双向认证和广播认证协议

双向认证又叫互认证，不同于单向认证，它需要通信双方都向彼此证明自己的身份。

1. 基本认证协议

执行单向认证 2 次可以做到相互认证，但这时的 2 次操作并没有什么逻辑联系。下

面算法可以解决这个问题,并减少了相互交换的信息数量。当然,采用数字签名再进行相识的认证操作也能做到互认证。

(1) B 发送一随机数 r_B 给 A。

(2) A 计算出 $M_A:=\mathrm{MAC}(r_B \| r_A, K)$,并发送 M_A、R_A 给 B。

(3) B 验证 M_A 是否等于 $\mathrm{MAC}(r_B \| r_A, K)$,并计算 $M_A:=\mathrm{MAC}(r_B \| r_A, K)$,然后发送给 A。

(4) A 验证 M_A 是否等于 $\mathrm{MAC}(r_B \| r_A, K)$。

2. 基本广播认证协议

广播认证是一方广播的信息被多方认证的过程。由于在对称协议中是预置密钥对,而在非对称协议中是每个实体有公/私密钥对。因此,基本的广播认证协议是采用基于非对称密码学的数字签名来进行信息认证。

3. 非对称 MAC 广播认证

非对称 MAC 广播认证协议最初由 Canetti 提出,该协议通过采用对称 MAC 来达到采用数字签名的非对称效果。首先要有一密钥群,每一个实体在初始化时都有较高的密钥子群,预置的密钥子群必须保证任何 2 个实体都有较高的拥有至少 1 个相同密钥的可能性。这种方法相对数字签名来说有较快的计算速度,但由于其过高的信息负载,所以不适用于带宽受限的无线传感器网络。

14.3.4 高级认证协议

1. Lamport 一次性口令协议[7]

该协议是采用 Hash 链的方法。首先,A 随机产生一个口令 w。其次,用散列函数 h 得出一系列口令 $w, h(w), h(h(w)), \cdots, h^t(w)$。其中,$h^t(w)$ 表示迭代了 i 次散列函数 h 之后得出的口令;$W_i=h^{t-i}(w)$ 表示第 i 次用来认证的口令。算法步骤如下:

(1)初始化阶段。A 以可信的方式传送 w 给 B,B 保存 w,并初始化它的计数器 $j \leftarrow 1$。

(2) for 每一次认证 $i=1$ 直到 $i=t$ do。

(3) A 发送 w, i 给 B。

(4) B 验证 i 是否等于 j,同时验证 $h(w)$ 是否等于 w。如果都相等,B 保存 w 并置计数器 $j \leftarrow j+1$,为下一次会话作准备。

(5) end for。

2. TESLA 协议[8]

TESLA 协议是一种信息广播认证协议。最初主要适用于因特网认证,它与非对称 MAC 协议一样没有采用高计算量的公钥算法,但它通过引入时间同步分段的机制解决了非对称 MAC 协议信息负载过高的问题。

发送方 A 产生一个散列密钥链 k_n, $k_{n-1}=h(k_n)$, $k_{n-2}=h(k_{n-1})$, $\cdots$, $k_0=h(k_1)$。首先,A 通过安全渠道〔如采用一次数字签名)把 K_0 广播给所有接收者;其次,A 发送时间段 t_i 的信息 m_i,就是说 m_i 只能在时间段 t_i 内才能被接收;最后,A 在下一个时间段 t_{i+1} 再公布 k_i,同时接收方用验证上一时间段接收到的 m_i。

认证算法如下:接收方必须先缓存信息然后才能再处理信息,另外,还需要发送方和接收方时间上同步;在密钥公布后,就给恶意攻击者用该密钥伪造信息创造了机会。因

此，在这种认证协议运行的同时，还需要另一认证协议来保证时间同步的真实性。在无线传感器网络中有该协议的一个改进版 μTESLA 协议。

3. Guy Fawkes 协议[9]

该协议采用单向散列函数来实现密钥承诺的办法来进行信息认证，算法如下：

(1) A 随机产生一个密钥 k_0 并发送 $h(k_0)$ 给 B。

(2) for 对于信息 m，i 从 1 到 n do。

(3) A 选择一个密钥 k_i 并承诺 $a_i := \mathrm{MAC}(m_i \parallel h(k_i), k_{i-1})$。

(4) A 公布 a_i。

(5) A 发送 $(m_i, h(k_i), k_{i-1})$ 给 B。

(6) B 验证 a_i 是否等于 $\mathrm{MAC}(m_i \parallel h(k_i), k_{i-1})$，并用上一个循环获得的 $h(k_{i-1})$ 验证 k_{i-1} 是否就是上一个循环所承诺的密钥。

该广播认证协议没有采用 Hash 链，而是采用承诺链的办法，即每个认证信息都包含一个下一步认证所需的密钥的承诺（$h(k_i)$ 代表这个承诺）。这个协议需要两个条件：一是 A 让 a_i 是公开的；二是 A 要知道 B 接收到了 a_i。

4. 远程用户认证[10]

远程用户认证是保证远程用户合法使用本地信息的认证协议。首先，在初始化阶段 A 发给 B 一个随机数据流 x，同时发送一系列由密钥 k_i 计算的 MAC 集合 $S := \{\mathrm{MAC}(x, k_i)$ 对应所有的 $k_i\}$。在第一次的验证阶段，A 产生一个新的密钥集 k'_i 和对应的 MAC′ 集。然后，这两套密钥集反复利用。A 通过证明其知道密钥子集来获得 B 的认证。其认证算法如下：

(1) 初始化阶段，A 产生一个随机密钥集 k_i，$i \in S$ 和一个随机数据流 x，并发送所有的 $U_i := \{\mathrm{MAC}(X, k_i)\}$ 给 B。

(2) for 认证阶段 j do。

(3) A 产生随机密钥集 k'_i 和一个随机数据流 X'，并计算所有的 $U'_i := \mathrm{MAC}(X', k'_i)$，然后发送所有的 $W_I := \mathrm{MAC}(U'_I, k'_i)$ 给 A。

(4) B 选出一个子集 $S' \in S$ 并发给 A。

(5) A 发送 S' 对应的密钥子集 k_i 和所有的 U'_i，X' 给 B。

(6) B 验证子集 $U_i, i \in S$ 并验证 $W_i, i \in S$。

(7) B 置 $X \leftarrow X'$ 和 $U_i \leftarrow U'_I$，A 置 $k_i \leftarrow k'_i$ 为下一次认证作准备。

(8) end for。

目前主要安全协议性能评估如表 14.1 和表 14.2 所列。其中，“-”表示协议不需要改需求；“x”表示需要；“+”表示有此功能。低能耗和低带宽由 4 个级别：“- -”表示该协议只能在能量充足的节点上运行；“+ +”表示该协议能量损耗使极小的。

表 14.1　认证协议需求与功能分析

认证协议	协议需求				协议功能		
	安全转发	预制密钥	TTP/PKI	时间同步	实体认证	单双信息认证	广播认证
数字签名	-	-	x	-	+	+	+
混合型认证	-	-	x	-	+	+	+

（续）

认证协议	协议需求				协议功能		
	安全转发	预制密钥	TTP/ PKI	时间同步	实体认证	单双信息认证	广播认证
对称服务器	-	x	x	-	+	+	-
MAC	-	x	-	-	+	+	-
时间标记(MAC)	-	x	-	x	+	+	-
非对称 MAC	-	x	x	-	+	+	+
TESLA	-	-	x	x	+	+	+
Lamport	x	-	-	-	-	+	-
Guy Fawkes	x	-	-	-	-	+	-
远程用户认证	x	-	-	-	+	+	-

表 14.2　认证协议效能分析

认证协议	低能耗	低带宽	认证协议	低能耗	低带宽
数字签名	- -	+	非对称 MAC	+	- -
混合型认证	-	-	TESLA	-	+ +
对称服务器	+	+	Lamport	+ +	+ +
MAC	+ +	+ +	Guy Fawkes	+ +	+ +
时间标记(MAC)	+ +	+ +	远程用户认证	+ +	- -

从表 14.1 和表 14.2 中可以看出，有些认证协议已经具备直接运用到传感器网络上的条件，有些则需要改进则可能可以适用。

14.4　无线传感器网络密钥管理机制

14.4.1　密钥管理基础

密钥管理是无线传感器网络安全机制的一个研究热点，无线传感器网络存在着和传统网络一样的安全目标，其安全特性如下：

(1)可用性。可用性是指网络服务对用户而言必须是可用的，即使是受到攻击，节点仍然能在必要的时候提供有效的服务。可用性保证网络正常服务操作并能容忍故障，即使存在相关的攻击威胁。在网络层中，攻击者可以删除会话级安全信道中的加密；在应用层，密钥管理服务也可能受到威胁。拒绝服务可以在各个层进行，使节点无法获得所需的正常服务。同时，可用性还涉及到能源问题，一旦没有能源节点将完全瘫痪。为了节省能量，通常会考虑让节点在空闲的时候处于睡眠状态，而在必要时将其唤醒。但是，攻击者可以设法通过某种合法的方式与节点交互，使其始终处于通信状态，目的是消耗节点的有限能量。这种攻击称为剥夺睡眠攻击，与其他攻击相比，这种攻击可能更为致命。因此需要通过强认证机制来确保通信对端的合法性。

(2)机密性。机密性是指保证特定的信息不会泄露给未授权的用户。军事情报或用户账号等安全敏感信息在网络传输时必须是可靠的、机密性的，否则这些信息被敌方或恶

意用户捕获，尤其是路由信息也需要保密，因为这些信息可能被敌方用来识别和确定目标在战场上的位置。该问题的解决需要借助于认证和密钥管理。

(3)完整性。完整性是指保证信息在发送的过程中不会中断，且保证节点接收的信息与发送的信息完全一样。如果没有完整性保护，网络中的恶意攻击或无线信道的干扰都可能使信息遭到破坏而变得无效。

(4)认证。一个移动节点需要通过认证来确认与它通信的节点身份，即是否为己方节点。如果没有认证，恶意攻击者就可以假冒网络中的节点来和其他节点进行通信，那么，他就可以获得那些未被授权的资源和敏感信息，并以此威胁整个网络的安全。

(5)不可否认性。不可否认性即抗抵赖性，它用来确保一个节点不能否认它已发出的信息。它对检查和孤立被攻击的节点具有特别的意义。当节点 m 接收来自被俘获的节点 n 的错误信息后，不可否认性保证节点 m 能够利用该信息告知其他节点 n 已被俘获。此外，不可否认性对于无线传感器网络军事应用中保证用户否认利害程度是至关重要的。

(6)敏感性。无线通信方式的使用使得无线传感器网络对于链路攻击从侦听到攻击都特敏感。侦听使恶意攻击者可以访问秘密信息，违背了机密性。攻击使得恶意攻击者可以删除、插入、修改信息，从而违背了可用性、完整性和可验证性。

(7)薄弱性。由于无线传感器网络物理保护相对薄弱，因此不应只考虑网络外部的恶意攻击，还应考虑来自内部的有意或无意的损坏与攻击。

(8)可扩展性。无线传感器网络是动态的网络，网络中的节点会因为能量的因素而不断地脱离网络，或者因为需要而加入网络，网络拓扑结构的动态性使网络不断饱和化。因此，安全机制必须是可扩充性的。

14.4.2　密钥管理模型

密钥的建立和管理过程是无线传感器网络安全首要面对和解决的问题。由于无线传感器网络计算和能量的限制，使非对称密钥的很多算法（如 Diffie - Hellman 密钥协商算法）无法在无线传感器网络下实现，只能考虑使用对称密钥的协商和管理协议。除此以外，传感器网络在协商密钥时，还应减少数据冗余等来降低密钥协商时的通信量。

依据网络体系结构的不同，密钥管理可以分为两大类：分布式密钥管理和分簇式密钥管理。针对分布式网络结构，目前已经提出的模型有预置全局密钥、预置所有对密钥、随机预分配密钥、Q-composite 随机密钥预分配模型、多路密钥增强模型、随机密钥对模型、对密钥预分配模型等。预置全局密钥的密钥管理模型是由 Bocheng 等人首先提出的[11]，这是最简单的密钥管理方案。针对分簇式网络结构，目前已经提出的模型有基于 KDC 的对密钥管理模型、低能耗密钥管理模型、轻量级密钥管理模型等。

依据共享密钥的节点个数，无线传感器网络密钥管理方法可以分为对密钥管理方案和组密钥管理方案；依据密钥产生的方式，可分为预共享密钥模型和随机密钥预配置模型。此外，还有基于位置的密钥预分配模型、基于密钥分发中心的密钥分配模型等。

1. 预共享密钥分配模型

预共享密钥主要有两种方式：节点之间共享和每个节点与 Sink 节点之间共享。预共享的密钥分配方法实现简单，适用于规模不大的应用网络。预共享密钥模型中，使用每对

节点之间共享一个主密钥，显然可以在任何一对节点之间建立安全通信，但其扩展性、抗俘获能力都很低，而且网络的规模不宜过大。在每个节点和 Sink 节点之间共享一个主密钥，使得每个节点的存储空间需求大大降低，但整个网络过分依赖 Sink 节点，计算和通信的负载都集中在 Sink 节点上容易形成整个网络的瓶颈。典型的使用预共享密钥的方式来建立安全连接的算法是 SPINS[2]。

2. 预置所有对密钥的密钥管理模型

该模型是由 Sanchez 等人提出的[12]，其主要思想是在网络部署前首先由离线密钥服务器生成 $N(N-1)/2$ 个密钥，其次，将任意 2 个节点 i,j 对应的不同的密钥组成密钥对 $K_{i,j}$，最后将密钥分别存入每个节点，每个节点所存储的密钥数为 $N-1$ 个。该模型的优点是由于网络中的通信不依赖于基站，所以网络的灵活性比较强。而且网络通信负载较少，计算复杂度低。模型缺点是支持网络的规模小，网络的扩展性不好。预置密钥流程如图 14.2 所示。

3. 随机密钥预分配模型

基本的随机密钥预分配模型是由 Eschenauer 和 Gligor 首先提出的[13]，其主要思想是为每个传感器网络选择一个比较大的密钥空间(又称密钥池)，任何节点都从密钥池中随机地选取并保存 M 个密钥，并保证任意两个节点共享同一个密钥的概率大于 P_m。每个节点公布它保存的所有密钥的 ID，并记录所有与它有共同密钥的节点。如果它要与某个节点建立连接，可以先查看这两个节点是否共享相同的密钥，如果密钥相同，则用这个密钥来作为会话密钥；如果密钥不同，则由源节点产生个会话密钥，通过互相共享密钥的邻居节点建立一条安全路径，将这个会话密钥传给目标节点。密钥路径建立如图 14.3 所示。

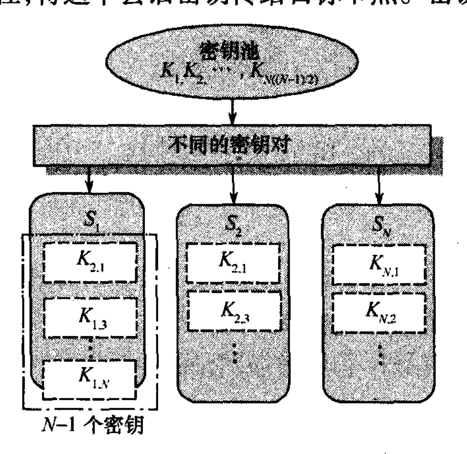




图 14.2　预置密钥流程

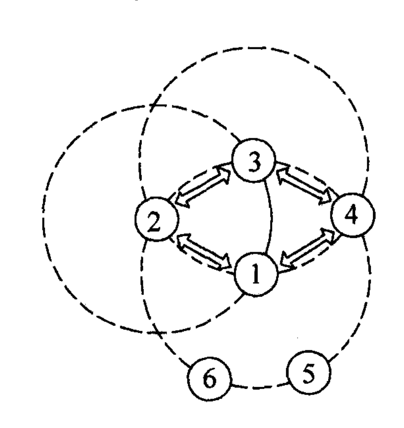


图 14.3　密钥路径建立

Q-composite 模型将基本的随机密钥预分配模型中的两个节点公共密钥最低要求提到了 q_m 个，以提高系统的抵抗力。在此方案中，获得了所有共享密钥信息以后，如果两个节点之间共享密钥数量超过 q_m 个，那么就由共享的密钥生成一个主密钥，作为两个节点的共享主密钥，提高 q_m 值意味着缩小整个密钥池的大小，但这样也会使得敌人俘获少数几个节点就能恢复很大的密钥空间，因此寻找一个最佳的密钥池大小是 Q-composite 模型的关键。

结合基于矩阵的密钥对预分配算法和密钥空间的概念，多密钥空间的密钥对预分配

模型生成多个基于矩阵的空间(矩阵池),从而为每个节点存放 t_m 个密钥空间的密钥对矩阵行。这样两个节点以一定的概率不共享某个密钥空间(某个矩阵),从而能够计算出其共享的会话密钥。

4. 基于位置的密钥预分配模型

基于位置的密钥预分配方案是对随机密钥预分布模型的一个改进。这类方案在随机密钥对模型的基础上引入了传感器节点的位置信息,每个节点都存放一个地理位置参数,基于位置的密钥预分配方案借助于位置信息,在相同网络规模、相同存储容量的条件下,可以提高两个邻节点具有相同密钥对的概率,也能够提高网络节点抗击被俘获的能力。

Liu 的方案[14]把传感器网络划分为大小相等的单元格,每个单元格共享一个多项式。每个节点存放其所在单元格及相邻 4 个单元格的多项式,周围节点可以根据自身坐标和该节点坐标判断是否共同具有相同的多项式。如果具有相同的多项式,就可以通过多项式计算出共享密钥对,建立安全通信信道;否则,可以考虑通过已有的安全通道协商共享密钥对,此方案需要部署 Sink 节点帮助确定节点的期望位置及邻节点,并为其配置共享多项式。

Huang 的方案[15]是对基本的随机密钥预分配方案的扩展。它把密钥池分为多个子密钥池。每个子密钥池又包含多个密钥空间。传感器网络被划分为二维单元格,每个单元格根据位置信息对应一个子密钥池。每个单元格中的节点在对应的子密钥池中随机选择多个密钥空间。尤其不同的是,该方案为每个节点选择其每个相邻单元格中的一个节点,并部署与其共享的秘密密钥。这样每个单元格中的每个节点都被分配了唯一的密钥,由此,网络节点具有更强的抗俘获能力。

基于对等中间节点(Peer Intermediary)的密钥预分配方案[16]是一种基于位置的密钥预分配方案。它的基本思想是把部属的网络节点划分成一个网格,每个节点分别与它同行和同列的节点共享密钥对。对于任意两个节点 m_m 和 n_m 都能够找到一个节点 k_m,k_m 分别和 m_m、n_m 共享秘密的会话密钥,这样通过 k_m、m_m 和 n_m 就能够建立一个安全通信信道。此方案大大减小了节点在建立共享密钥时的计算量及对存储空间的需求。

5. 多路密钥增强模型

多路密钥增强的思想最初是由 Anderson 和 Perrig 提出来[17],而 Chan-Perrig-Song 提出的多路密钥增强模型[18]是在随机密钥预分配方案的基础实现的,该方案的主要思想是在多个独立的路径上实现密钥更新,以增强节点被俘获后增强网络的自恢复能力。

6. 对密钥预分配模型

Wenliang Du 等人提出了对密钥预分配模型[19],该模型是建立在 Blom 的密钥预分配方案[20]的基础上并联合了随机密钥与分配模型的方法。Blom 的方案没有考虑无线传感器网络这样的应用,虽然可以达到让网络拓扑实现安全连接,但对节点的资源开销占用极大。其主要思想是让网络中的任一对节点可以找到共享密钥对,且只要俘获节点的数目未达到门限值网络就是安全的。其具体实施分为密钥预分配阶段和密钥协商两个阶段。

7. 基于 KDC 的组密钥管理模型

基于 KDC 的组密钥管理[21]主要是在逻辑层次密钥(Logical Key Hierarchy, LKH)方案上的扩展,如 Routing Awared Key Distribution Scheme 方案和 ELK 方案。这些密钥管理模型要求普通传感器节点的计算量较少,不需要占用大量内存空间,有效地实现了密钥的

前向保密和后向保密，并且可以利用 Hash 方法减少通信开销，提高密钥更新效率。但在无线传感器网络中，KDC 引入异构化了网络结构，增加了网络的脆弱环节，KDC 的安全性直接关系到网络的安全。另外，KDC 与节点距离甚远，节点要经过多跳路由才能到达 KDC，会导致大量的通信开销。因此，基于 KDC 的密钥模型不是无线传感器网络密钥管理的理想选择。基于 KDC 模型的密钥会话流程如图 14.4 所示。

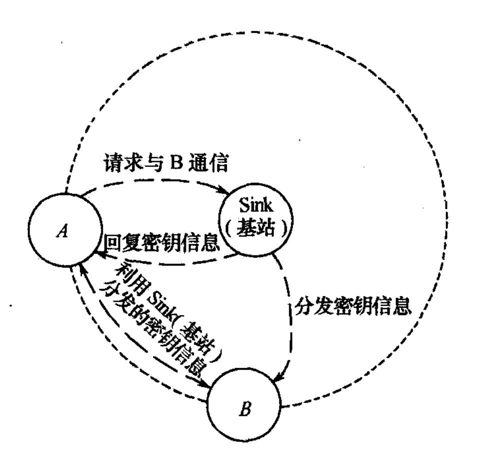


图 14.4　基于 KDC 模型的密钥会话流程

8. 低能耗密钥管理模型

低能耗密钥管理模型[22]是由 Jolly 等人提出来的。它是基于 IBSK 协议[23]扩展而来的，继承了 IBSK 支持增加、删除节点以及密钥更新的优点，同时为了减少能量的消耗，取消了节点与节点之间的通信。由于目前一些技术的限制，所以该协议是在一些假设的基础上进行的。首先假设基站有入侵检测机制，可以检测出节点正常与否，并由此决定是否出发删除节点的操作。该模型对传感器节点不作任何信任的假设，簇头之间可以通过广播或单播与节点通信。该模型包括 3 个阶段：预分配阶段、初始化阶段和增加新节点阶段。

9. 其他密钥管理方案

其他密钥管理模型，如 Multipath Key Reinforcement Scheme 和 Using Deployment Knowledge 等，应根据具体的应用来选取合适的密钥管理方案。目前，大多数的预配置密钥管理机制可扩展性不强，而且不支持网络的合并，网络的应用受到局限；而且在资源受限的网络环境，让传感器节点随机性地和其他节点预配置密钥也不是一个高能效的选择。因此与应用相关的定向动态的密钥预配置方案将获得更多的关注。

14.5　网络入侵检测技术

14.5.1　入侵检测需求

在无线传感器网络中，入侵预防技术已经得到了广泛的认可，如加密、认证、标签等。但单独使用加密、认证等入侵预防技术往往是不够的，并且安全机制的引入会使得系统变得更加复杂，暴露的弱点也更多，系统的稳定性和可靠性也会随之降低，从而将导致更多的安全问题出现。同时在无线传感器网络中，由于其几乎不依赖于任何固定基础设施，使得防火墙方案完全不能适用。如何保护网络的安全，提高网络的安全防御性能，成为无线传感器网络中一个急待解决的问题。入侵检测可以用作网络防御的第 2 道防线，一旦检测到入侵企图或已经发生的入侵活动，即引发相应的响应以阻止或减少系统的损害。

借鉴传统的入侵检测系统，考虑无线传感器网络的网络特性，无线传感器网络入侵检测技术大致应包括 13 个方面的内容：

(1)检测的数据源。

(2)使用基于误用和异常的混合模型的检测技术。

(3)检测的方式。采用集中检测还是分布式检测。

(4)检测频率。采用间断还是连续的方式。

(5)反应机制。

(6)不能引入新的系统安全漏洞。

(7)不能消耗和占用太多的资源,如能源、CPU、内存、带宽等。

(8)攻击检测需要采用合适的间断机制。

(9)IDS 能够基于“部分的”和“本地的”信息行为进行检测。

(10)可靠性要高。

(11)具有良好的扩展能力。

(12)本地局部检测与全局检测相结合。

(13)路由负载增加适度,能保证或不影响正常的网络性能。

由于无线传感器网络的任何协议和安全机制都要以能量有效性为前提,因此入侵检测系统必须采取简单高效的设计,以降低节点间过多的通信、计算开销。

目前,传感器网络的实用领域和范围还相当有限,规模引入相对较小,网络安全性要求还没有达到类似互联网和 Ad hoc 移动自组网所具有的防御机制。随着无线传感器网络越来越广泛的应用,新的攻击类型也将会迅速增加,仅仅使用基于规则的检测技术只能检测到少数已知的攻击类型,因此,无线传感器网络的攻击检测应主要采用异常检测技术。同时,为了减少攻击节点带来的损失,无线传感器网络的攻击检测机制应能尽早发现并隔离攻击节点。

14.5.2　入侵检测基础

众所周知,不管在网络中采取多么先进的安全措施,攻击者总有可能找到网络系统的弱点,实施攻击。单独使用加密、身份验证(如用户名、口令)等预防技术很难达到预期的安全指标。这些技术可以降低网络被攻击的可能性,但是无法杜绝攻击,因此,安全的防御手段也是不可或缺的。针对网络安全防范措施的不足,入侵检测系统(Intrusion Detection System,IDS)应运而生,它可以为网络安全提供实时的入侵检测,并及时有效地采取相应的保护。

14.5.2.1　入侵检测技术原理

入侵检测技术作为一种主动的入侵防御技术,已经发展成安全网络体系中的一个关键性组件。其积极、主动的防御思想,完全区别于加密、认证、防火墙等传统的被动防御方案,入侵检测技术正在引领网络安全从被动走向主动。

入侵行为被定义为任何破坏目标的机密性、完整性和可访问性的动作,入侵一般可分为外部入侵和内部入侵。外部入侵借助一定的攻击技术对攻击目标进行监测、查漏,然后采取破坏活动;内部入侵通常利用社会工程学盗用非授权账户进行非法活动,有统计表明,入侵行为有 80% 来自内部。

入侵检测的研究最早可以追溯到 Anderson James P. 在 1980 年为美国空军作的题为“Computer Security Threat Monitoring and Surveillance(计算机安全威胁监控与监视)”的技术报告[24],其中,第一次明确阐述了入侵检测的概念,是该领城的开山之作。该报告提出了一种对计算机系统风险和威胁的分类方法,并将威胁分为外部渗透、内部渗透和不法

行为 3 种，提出了利用审计跟踪数据监视入侵活动的思想。该报告的理论成为入侵检测系统设计及开发的基础，成为基于主机的入侵检测系统和其他入侵检测系统的出发点。

Denning 在 1987 年所发表的论文中[25]，对入侵检测系统模式做出如下定义：入侵检测通过网络封包或信息的收集，检测可能的入侵行为，并能在入侵行为造成危害前及时发出报警，通知系统管理员并进行相关的处理措施。为了达成这个目的，入侵检测系统应包含 3 个必要功能的组件：信息收集、检测引擎和响应组件，如图 14.5 所示。



图 14.5　入侵检测系统简要构成图

目前，入侵检测已经发展成为一种动态的监控、预防或抵御系统入侵行为的安全机制。入侵检测技术是通过从网络或系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到入侵的迹象的一种安全技术。它在不影响网络性能的情况下能对网络进行监测，从而提供对付内部攻击、外部攻击和误操作的实时保护，提高了信息安全基础结构的完整性。入侵检测的软件与硬件的组合便是入侵检测系统。入侵检测可以分为实时入侵检测和事后入侵检测两种，两种攻击检测的原理如图 14.6 所示。

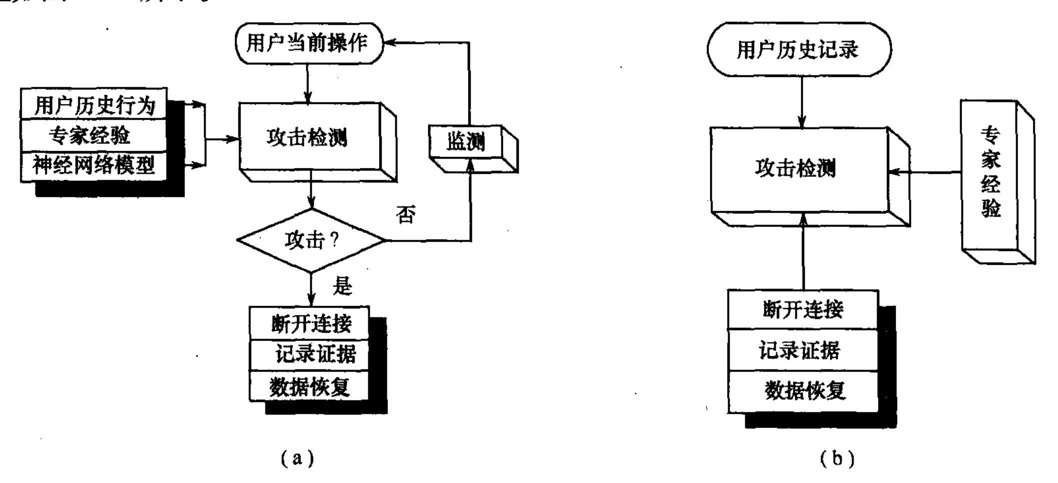


图 14.6　攻击检测原理

(a)实时攻击检测的功能原理；(b)事后攻击检测的功能原理。

实时入侵检测在网络连接过程中进行，系统根据用户的历史为模型、存储在计算机中的专家知识、神经网络等模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的联系。在无线传感器网络中完成这一功能的节点主要是 Sink 节点，当然传感节点也参与进行检测，只是依据自身的资源限制，运行简单而有效的专家知识。

事后入侵检测由网络管理机构进行，通过系统而全面的知识，根据历史审计记录判断入侵检测行为是否存在。这种方法分为定期和不定期，不具有实时性。

14.5.2.2　一种通用的入侵检测模型

研究一种技术或系统的基本方法是分类，入侵检测按其实现中的各种不同要素可进

行不同的分类。

根据数据信息来源进行分类，主要有基于网络的 IDS、基于主机的 IDS 和混合型的 IDS（将基于主机和基于网络的入侵检测系统相结合）。

根据响应方式的不同，入侵检测系统可以分为主动响应 IDS 和被动响应 IDS。

根据系统各个模块运行的分布方式不同，入侵检测分为集中式入侵检测和分布式入侵检测。

根据数据分析方法即检测方法的不同，可将入侵检测系统分为异常入侵检测（Anomaly Detection）和误用入侵检测（Misuse Detection）。

目前，较为通用的入侵检测模型是将异常检测和误用检测相结合的模型。

1. 异常入侵检测

该方法先总结正常操作应该具有的特征（如特定用户的操作习惯与某些操作的频率），并得出正常操作的模型，在后续的操作检测过程中，一旦发现偏离正常统计学意义上的操作模式，即进行报警。基于异常的入侵检测多采用统计、专家系统、数据挖掘、神经网络和计算机免疫等技术。

2. 误用入侵检测

该方法的特点是收集正常操作，即入侵行为的特征，建立相关特征库，在后续的检测过程中，将收集到的数据与特征库中的特征代码进行比较，得出是否是入侵的结论。基于误用的入侵检测主要采用专家系统、模型推理、状态迁移分析、模式匹配等技术。

基于异常的入侵检测系统的优点是能发现一些未知的攻击，对具体系统的依赖性相对较小，但误报率很高、配置和实现也相对困难；基于误用的入侵检测能比较准确地检测到已经标识的入侵行为，但是对具体的系统依赖性太强、移植性不太好，而且不能检测到新的攻击类型。因此，最佳的解决途径就是将两者有机结合起来，以得到更为高效的入侵检测伸展性能，模型如图 14.7 所示。

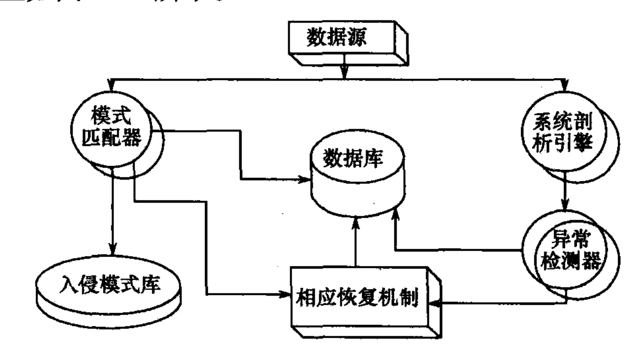


图 14.7　一种通用的入侵检测模型

14.5.3　几种入侵检测方案

在无线传感器网络入侵检测的研究中，已有的理论成果相对较少。目前，已经提出了一些较好的入侵行为检测算法[26~28]，如博弈论框架、马尔科夫判定过程 MDP、依据流量的直觉判定、分布式贝叶斯算法、针对无线传感器网络的入侵检测模型等，然而这些研究大部分仅处于模型设计、理论分析和仿真试验的阶段。

1. 博弈论框架

基于博弈论的无线传感器网络框架[27]，把攻击—防御问题视为在攻击者和传感器网络之间两个博弈者的非零和、非协作博弈问题，由此所产生的博弈机制作为网络的防御策略，其结果是趋于纳什均衡的[26]。博弈论框架可大大提高传感器网络防御入侵的成功率，是较为高效的一种入侵检测防御机制。

对于一个固定的簇 k，攻击者有 3 种可能的策略：AS1 攻击群 k、AS2 不攻击群 k、AS3 攻击其他群。IDS 也有两种策略：SS1 保护簇 k 或者 SS2 保护其他簇。

因此，存在两个矩阵：IDS 付出矩阵 $\boldsymbol{A}$ 和攻击者付出矩阵 $\boldsymbol{B}$。这两个博弈者的支付关系用一个 2×3 的矩阵表示，矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 中的 a_{ij} 和 b_{ij} 分别表示 IDS 和攻击者支付。

IDS 付出矩阵 $\boldsymbol{A}=(a_{ij})_{2\times3}$ 定义为

$$\boldsymbol{A}_{ij}=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \tag{14.1}$$

攻击者付出矩阵 $\boldsymbol{B}=(b_{ij})_{2\times3}$ 定义为

$$\boldsymbol{B}_{ij}=\begin{bmatrix} \mathrm{PI}(t)-\mathrm{CI} & \mathrm{CW} & \mathrm{PI}(t)-\mathrm{CI} \\ \mathrm{PI}(t)-\mathrm{CI} & \mathrm{CW} & \mathrm{PI}(t)-\mathrm{CI} \end{bmatrix} \tag{14.2}$$

式中：CW 为等待并决定攻击的所需成本；CI 为攻击者入侵的成本；$\mathrm{PI}(t)$ 为每次攻击的平均收益。

b_{11} 和 b_{21} 表示对簇 k 的攻击，b_{13} 和 b_{23} 表示对非簇 k 的攻击，它们均为 $\mathrm{PI}(t)-\mathrm{CI}$，表示从攻击一个簇所获得的平均收益中减去攻击的平均成本。同样，b_{12} 和 b_{22} 表示非攻击模式，若入侵者在这两种模式下准备发起攻击，那么 CW 就代表了因为等待攻击所付出的代价。

该方法也有弱点，即入侵检测成功率的波动性比较大，稳定性不够高，比较容易受其他因素的干扰。

2. 马尔科夫判定过程

用马尔科夫判定过程（Markov Decision Process，MDP）[28]来预测最脆弱节点。马尔可夫链就是假设在有限值范围内，存在随机过程 $\{X_n, n=0,1,2,\cdots\}$，如果 $X_n=i$，那么就说这个随机过程在时刻 n 的状态为 i。假定随机过程处于状态 a，那么随机过程在下一个时刻从状态 i 转移到状态 j 的概率为 p_{ij}。

基于过去状态和当前状态的马尔可夫链的条件分布与过去状态无关，而仅取决于当前状态。对 IDS 来说，可以给出一个奖励概念，只要正确选出予以保护的簇，它将为此得到奖励。MDP 为解决连续随机判定问题提供了一个模型，它是一个关于 (S,A,R,tr) 的四元组。其中，S 是状态集合、A 是行为集合、R 是奖励函数、tr 是状态转移函数。

如果既要考虑入侵检测的成功率，又要顾及入侵检测的稳定性，基于马尔可夫判定过程 MDP 的学习方案无疑是最佳选择。一种优秀的算法能够知道什么时候使用 MDP 方案，什么时候使用博弈论框架，从而使入侵检测的成功率达到最大。寻找这种算法是无线传感器网络领域未来研究的课题之一。

3. 依据流量的直觉判定

依据流量的直觉判定以直观判断的节点流量作为度量尺度[27]，保护具有最高流量值的节点。在一个时间片 IDS 必须选择一个簇进行保护，这个簇或者是前一个时间片内被保护的簇，或者重新选择一个更易受攻击的簇。通过定义"通信负荷"来表征每个簇的流量，IDS 根据"通信负荷"的参数大小选择需要保护的簇。所以在一个时间片内 IDS 应该保护的是具有最大流量的簇，这也是最易受攻击的簇。

4. 分布式贝叶斯算法

分布式贝叶斯算法是 Krishnamachari 等人针对区域容错行为提出的。该算法从可能的入侵进行统计，利用贝叶斯模型计算发生的概率，预测估计入侵发生的位置区域，给出了无线传感器网络入侵检测系统较好实施的设计思想，但没有解决攻击行为量化的问题。

针对分簇型无线传感器网络，Su 等人提出了一种能量节省的入侵检测方案[30]。该方案针对簇头和普通的成员节点分别采用两种不同的检测方法：簇头负责监视簇内成员节点；成员节点监视其所在簇的簇头。并考虑因为担负着主要的通信任务，簇头的安全性相对更重要的实际情况，在选取监视它的成员节点时，综合考虑能量和安全性两个因素，只让符合选拔条件的成员节点参与对簇头的监视。

在设计整套方案时重点考虑了能耗问题，例如，它在解决对簇头的监视时，采用普通成员节点分组轮流工作的方法，但这样做同时也引入了更为复杂的组划分机制，增加了系统的复杂性和实施难度，对检测的准确率也会有一定的影响。

Edith Ngai 提出了一种针对无线传感器网络的入侵检测模型[29]，整个检测模型由邻居监测、数据融合、拓扑发现、路由追踪和历史记录几部分构成。并提出在邻居监测中使用 Watch-dog 方法，检测数据包的传输情况，认证错误节点；数据融合采用邻居节点间的本地融合和整个网络的全局融合相结合的方法。该入侵检测模型如图 14.8 所示。

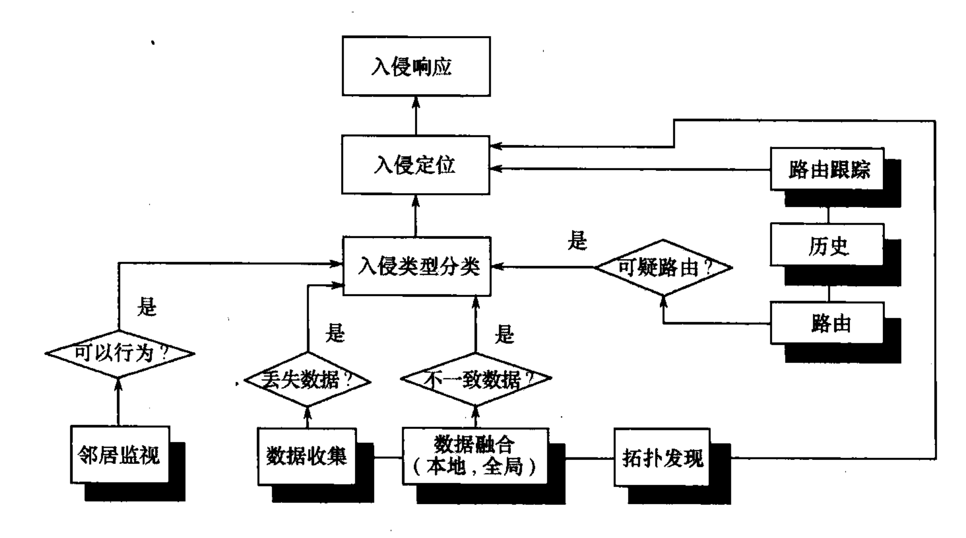


图 14.8　无线传感器网络攻击检测模型

Edith Ngai 提出的这种无线传感器网络的攻击检测模型，是将入侵类型的鉴别、入侵定位和响应机制结合在一起的一个完整的攻击检测响应模型，但对于如何具体的实现这种机制，以及许多技术问题没有做详细的考虑。

14.5.4 入侵检测研究方向

在研究无线传感器网络入侵检测时，一方面由于其与移动 Ad Hoc 网络有一定的相似性，因此可以参考 Ad Hoc 中现有的研究成果加以改进，使其适用于无线传感器网络的特殊要求；另一方面，要不断地探索和开发适合于无线传感器网络的新方法。

入侵检测模型是无线传感器网络入侵检测系统的重要研究内容。事实上，目前很多的研究也正是集中在这个方面，也已经提出了一些模型，如文献[29]中 Edith Ngai 提出的一种针对无线传感器网络的入侵检测模型，但这些模型都存在需要改进的地方。无线传感器网络需要的是经试验证明最有效的模型，因此模型设计还有许多问题需要进一步研究和解决。

在检测技术方面，入侵检测技术总体上可分为异常检测和误用检测两大类。考虑无线传感器网络计算、存储资源受限的特点，异常检测在其入侵检测领域应该有更多的优势。常用的异常检测技术有量化分析技术、基于传统统计方法的技术、基于(隐)马尔科夫过程的异常检测技术、基于神经网络的检测技术、基于免疫学的检测技术、基于遗传算法的检测技术和基于支持向量机的检测技术等。这些检测技术经过适当的改进(精简、优化)并能够适应传感器网络的要求后，都可以应用到无线传感器网络中来。需要注意的是，采用一种检测技术设计入侵检测系统的前提是不能有过多的资源消耗。

误用检测技术在有线网络中常见的有专家系统、攻击签名分析、状态转移分析、模式匹配等。由于采用误用检测技术的系统一般都过于庞大，而且需要完备的数据库的支持，因此，相对于无线传感器各种资源严格受限的实际来说，其应用有一定的局限性。但是，由于其检测的准确率一般比较高而且可以鉴别攻击的类型、误警率较低等优点，在实际应用中也可以通过一些改进，使其作为异常检测技术的补充应用到无线传感器网络中。例如，对能源不敏感的 Sink 节点上，可以采用异常和误用相结合的检测方案。

在检测机制方面，根据无线传感器网络节点构成和组网方式的特征，需要采用相应的检测机制，例如，文献[30]中 Su 等人针对分簇型无线传感器网络提出的检测方案，就是一个较好的方法。此外，由于 Sink 节点仍具有资源受限和数据瓶颈的问题①。目前，可以考虑将分布式计算中的移动代理(Mobile Agent)技术引入到无线传感器网络入侵检测中，通过移动代理实现入侵检测系统。

移动代理是一种独立的能够自主连续运行的软件实体，为解决复杂、动态、分布式智能应用提出的一种全新的计算手段。在无线传感器网络入侵检测中，使用 Agent 技术可以增加系统的可扩展性，解决数据与信息瓶颈问题，并可以改善单点失效带来的问题从而提高系统的容错能力。此外，Agent 能够自主地在各个主机之间移动，编程灵活、易于实现；可以根据需要动态地启动或停止，大大节省了系统的开销。尤其是对于缺乏基础设施的无线网络，使用该技术将会是一个很好的选择。

尽管移动 Agent 主要的缺点是会给参与者带来安全方面的威胁，但作为一种分布式的低消耗的计算模型，移动代理技术非常适合无线传感器网络的特殊需求，其在无线传感器网络入侵检测中的应用会成为今后研究的一个重要方向。

---

① 不能将传感器节点无法使用的任务或为减轻传感器节点的负担，将大量网络系统任务转交给 Sink 节点，其结果是造成 Sink 节点的数据瓶颈和信息瓶颈。

在无线传感器网络入侵检测中，入侵检测的目的不仅仅是要发现入侵，更重要的是要在发现入侵时能及时做出入侵响应。由于无线传感器网络本身比较脆弱，再加上各种资源受限、工作环境恶劣等特点使得其生命非常有限，恶意的攻击很可能造成网络的死亡，因此，响应机制特别是主动的响应机制，在无线传感器网络中是至关重要的。目前，有效的响应机制包括切断与恶意节点的通信、通知更新通信密钥、重新进行节点身份认证和通知基站采取人为干预等。及时准确地剔除恶意节点或找出攻击者，对于保证网络的正常运转和数据的安全性非常重要，入侵的定位技术也是未来的一个研究方向。

14.6 基于比较的多源网络簇节点故障判定算法

由于无线传感器网络应用环境的特殊性、无线信道不稳定以及能源受限的特点，传感器网络节点受损的概率远大于传统网络节点，因此，传感器网络必须具有健壮性，而网络故障判定对实时了解网络中的节点状态起着重要作用，以保障部分网络簇或节点的损坏不会影响全局任务的执行。

故障的网络节点被诊断出来，就能够把它们从传感器网络簇中分离出来，使其不影响到整个簇的运行。2001 年，意大利的 S. Chessa 和美国的 P. Santi 联合提出一种 Ad hoc 网络中基于比较的系统级故障诊断（Comparison-Based System-Level Fault Diagnosis，CBSLFD）算法[31]，该算法被称为相关领域第一篇研究网络故障诊断的文章。系统级故障诊断是指在由点到点的双向链路连接的网络节点组成的系统中，依据网络节点之间相互测试的结果实现故障诊断[32]。

CBSLFD 算法特点如下：

（1）对等诊断。

（2）通过泛洪的方式传递诊断信息，这种方式增加了无线通信介质的系统带宽开销，同时大量的计算也造成了网络节点能量有效性的降低。

（3）存在重复诊断，重复诊断不符合无线传感器网络能量有效性要求。

（4）研究基础是网络拓扑不变的故障诊断。当拓扑发生变化时，部分节点的状态将无法确定。

借鉴 CBSLFD 算法的优点，本节利用分层型网络中的簇及其簇内节点和 Sink 的链路关系，提出了基于比较的多源网络簇节点故障判定（Comparison-Based Cluster Nodes Fault Diagnosis，CBCNFD）算法。

14.6.1 节点故障判定系统模型[33,34]

CBCNFD 算法利用簇头作为簇内故障判定的集中控制单元对簇内节点进行集中判定，同时，利用链接所有簇头的逻辑子网，通过在簇头之间传递相关判定信息的判定方式，对簇头进行判定。CBCNFD 算法既适用于网络拓扑固定的节点，又适用于网络拓扑变化的节点。同时解决了网络节点的重复诊断，尤其是在网络规模较大，分簇较多的情况下，CBCNFD 算法可以大大降低网络系统的开销。

14.6.1.1 CBCNFD 算法模型

用 CBCNFD 算法进行诊断的无线传感器网络由 n 个移动节点组成，在 t 时刻，网络系

统拓扑可以描述为无向图 $G(t)=(V,L(t))$，称之为网络系统拓扑通讯图。V 是该网络中所有节点的集合，$L(t)$ 是 t 时刻的逻辑链路集合。对于任意的节点 $u,v\in V$，当且仅当 v 在 t 时刻位于 u 的通信范围之内时，有 $(u,v)\in L(t)$。如果 u 与 v 在 t 时刻相邻，那么，t 时刻与 u 相邻的节点集合为 $N(u,t)$。

模型同时满足以下规则：

(1) 每一个网络簇节点有唯一的标识(IDentity)，所有节点被排序并按照序数进行标识。

(2) 存在链路层协议提供的服务。在逻辑连接上有 MAC 协议解决广播信道的多址问题；提供简单的一跳可靠广播(1 - hop reliable broadcast)，记为 1_rb(・)，在集合 $N(u,t)$ 内，t 时刻的消息 m 被节点 u 所调用，消息 m 可以被正确传递到所有节点；每个移动节点都知道其邻居的身份；消息接收者知道消息发送者的身份。

(3) 网络成簇算法。位于簇头通信范围内所有节点都属于同一个簇，簇内所有节点都是簇头的一跳邻居；簇头和簇头之间不互为邻居；簇头和簇头之间通过 Sink 链接，或通过其他簇间接链接；簇头知道整个网络中共有多少节点及其各自的标识；在网络节点诊断过程中，簇头不发生改变，如图 14.9 所示。

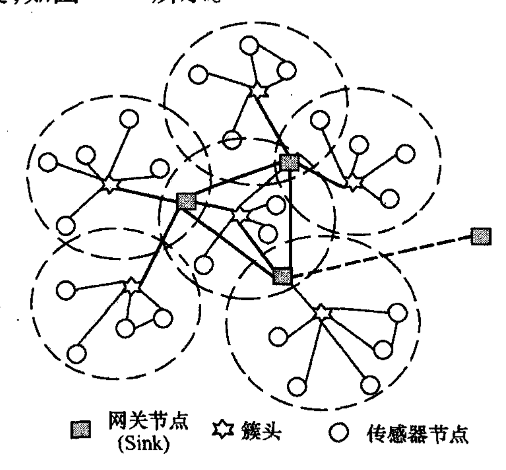


图 14.9　成簇算法图例

CBCNFD 算法使用的网络拓扑数学模型为式(6.2)～式(6.4)，使用该数学模型可以在保证应用需求的前提下，使网络数据传输量最小且链路负载最小[35]，一方面可有效降低网络系统能耗，一方面可有效提高网络利用数据的实时性，为故障判定算法提供能源和实时性指标。

14.6.1.2　故障模型

网络节点有正常和故障两种状态，故障是"永久的"。例如，一个故障节点将持续故障直到该节点被维修或替换。故障包括硬故障和软故障：硬故障节点无法和网络簇中其他节点通信，在无线传感器网络中，硬故障主要是节点损毁和电源不足造成的；软故障节点尽管与上层应用有关的工作状态不正常，但可以继续运转并与簇内其他节点进行通信。为了实现诊断的需求，软故障节点的行为被有所限制，因此本文采用 gMM(generalized Maeng and Malek)[36]模型作为失效规则。在 gMM 模型中，由测试任务节点 u 发起诊断信息，该信息分发到相邻的一对节点 v、w，通过 v、w 节点间的比较得到诊断结果。该规则描

述如表 14.3 所列，如果 u、v 和 w 都是正常，那么比较的结果“一致”，比较输出为“0”；如果 u、w 任何一个故障，那么比较结果“不一致”，比较输出为“1”。

表 14.3　gMM 失效规则

u	v	w	由 u 发起，v 和 w 的比较结果
正常	正常	正常	0
正常	故障	正常	1
正常	正常	故障	1
正常	故障	故障	1
故障	任意	任意	没有结果

14.6.2　网络簇节点故障判定模型

【引理 14.1】网络拓扑定义为无向图 $G=(V,E)$，V 表示网络中节点集，且满足 $1\leqslant |V|\leqslant g$，$g$ 为正整数，E 表示两个节点间的双向通信链路集。网络节点总数为 M，传感节点和簇头节点集合有 B 个节点，Sink 节点有 1 个。若 G 是连通的且 G 中故障网络节点总数不超过 $k(G)-1$，$k(G)$ 是 G 的连通度，则由 G 中任意网络节点产生的“分发消息”能够在有限时间内被 G 中所有的正常网络节点正确接收。

证明：设 G' 为正常网络节点集合组成的图，且 $G'\subset G$。由于故障节点总数小于 $k(G)$，因此 G' 也是连通的，对于 G 中任意给定的正常网络节点 u、v，存在一条从 u 到 v 的路径 h，h 为有效路由的网络节点连通路径，$l(h)$ 为路径 h 的长度。设在设定时间内，u 产生的一个分发消息 m 可被 v 正确地接收。

(1) $l(h)=1$。设 v 是 u 的邻节点，由成簇算法提供可靠的一跳广播，m 通过虚拟链路可将 m 正确发送到 v。若 u 已经被 v 判定为正常，则 m 被 v 正确接收；否则，u 尚未被判定，则保存 m，直到 u 最终被判定为正常。因此，$l(h)=1$ 时 m 能够被 v 正确接收。

(2) $l(h)=h$。设 w 为路径 h 上第 $h-1$ 个节点，则 w 是 v 的邻节点，且 w 已经正确接收到 m，w 依据 m 更新自身判定结果，并将 m 发给邻节点。因此，$l(h)=h$ 时 m 亦能被 v 正确接收。

【推论 14.1】设 G 是连通的，且 V 中故障节点总数不超过 $k(G)-1$，则每个正常簇头节点都能在有限时间内正确判定出 G 中所有簇头节点的状态。

【定义 14.1】设 $P_i=\{v_0,v_1,\cdots,v_{n-1}\}$ 为第 i 层中节点的集合，$i\in\{0,1,\cdots,n-1\}$，$C_i=\{v_{ij}\}$ 为第 i 个簇中的节点集合，则 $C=\{C_0,C_1,\cdots,C_{n-1}\}$ 为所有簇的集合。其中 v_{io} 表示簇头节点，v_{ij} 表示传感节点，显然有 $|P_i|=\sum_i |C_i|$。对于 P_i 层中的任意一个簇结构满足以下条件：

(1) $\cup_{i=1}^{n} C_i=P_i$，每一个节点分属不同的簇。

(2) $|C_i\cap C_j|=\phi$，任两个簇之间没有交集，即同一节点不能同属不同的簇。

(3) $|C_i|\geqslant 2$，任一个簇中的节点数目必须大于等于 2，且有一个簇头节点。

【引理 14.2】在无向图 $G=(V,E)$ 中，对于任意网络节点 u，$\exists C_i\in C$，使得 $T_i>T_s+T_{out}$，其中 T_i 为节点 u 在簇 C_i 内停留的时间，T_{out} 为定时器超时时间，T_s 为簇头节点检测到新节点并向其“发送测试请求”s 所需的时间上限，则任意正常簇头节点能够在有限时间

内获知网络中所有传感节点的状态。

证明：已知 $T_i > T_s + T_{out}$，则任意网络节点 u 在簇 C_i 内收到 s 后，必能在其离开该簇之前产生并发送 s，被簇 C_i 的簇头节点判定，进而任意簇内传感节点都将被网络中的某簇头节点判定，由引理 14.1，任意正常簇头节点能够在有限时间内获知网络中所有传感节点的状态。

由引理 14.1 和引理 14.2 可以确定，网络拓扑固定与改变两种情况下网络节点故障判定的原则如下：

【定理 14.1】在 t 时刻，设网络拓扑固定，正常节点 u 发出一个测试请求 s，则在 $t+T_{out}$ 时刻，节点 u 已经正确判定出在 $N(u)$ 中所有网络节点的状态，且任意正常节点 v 已经正确判定出在 $N(u)$ 中"正常"或"软故障"节点的状态。若 $N_u(z)$ 中至少有 2 个节点是正常的，则在 $N_2(u)$ 中的任意正常节点 z 已经正确判定出在 $N_u(z)$ 中的"正常"或"软故障"节点的状态。这里，$N_2(u) = \{z \in V - N(u) : |N_u(z) \geqslant 2\}$。

【定理 14.2】在 t 时刻，设网络拓扑发生改变，且 $N_s(u) = N(u,t) \cap N(u, t+T_{out})$，$N_s^x(u)$ 为 $N_s(u)$ 中正常或软故障节点。正常节点 u 发出一个测试请求 s，那么在 $t+T_{out}$ 时刻，节点 u 已经正确判定出在 $N_s^x(u)$ 中所有节点的状态。

14.6.3　故障判定模型评价标准

为了对本节规定的引理和定理有效性进行约束和判定系统性能进行综合评价，定义以下标准：

【定义 14.2】簇头节点故障判定处理过程通信复杂度为 $O(\max(n^2, \omega n))$，ω 复杂度系数。

(1)簇头节点互判定。任意给定正常簇头 z，簇头相互判定的过程中它最多产生"分发消息、发送测试请求和测试应答"的数量分别是 $n_{\max-m}=1$、$n_{\max-s}=1$ 和 $n_{\max-r}=\max|N(z,t) \leqslant d_{\max}|$，$d_{\max}$ 为 G 中节点度的最大值。z 最多转发 m 的次数为 $f_{\max-m}=n-1$。因此，在簇头节点相互判定过程中，簇头节点执行可靠一跳广播的次数为 $n(n+1+d_{\max})$。

(2)簇头节点判定静止传感节点。任意给定正常簇头节点 z，在簇头节点判定静止传感节点的过程中，所有簇头节点最多共产生"分发消息、发送测试请求和测试应答"的数量分别是 $n_{\max-m}=1$、$n_{\max-s}=1$ 和 $f_{\max-m}=n-1$，因此，簇头节点执行一跳广播的次数为 $n(n+1)$。

(3)簇头节点判定活跃传感节点。所有簇头节点最多共产生"分发消息、发送测试请求和测试应答"的数量分别是 $t_{\max-m}=\omega$、$t_{\max-s}=\omega$ 和 $t_{\max-r}=\max(\omega,\eta)$。任意给定正常簇头节点 z，有 $f_{\max m}=\omega$。因此，簇头节点执行一跳广播的次数为 $\max(\omega(n+2)+\eta, \omega(n+3))$。

【定义 14.3】簇内传感节点故障判定处理过程的通信复杂度为 $O(\max(l, \omega\eta))$。

【定义 14.4】Sink 节点故障判定处理过程的通信复杂度为 $O(\max(mn, \omega m))$。

【定义 14.5】整个传感器网络故障判定处理过程的通信复杂度为 $O(\max(n^2, \omega n, mn, \omega m, l, \omega\eta))$。

【定义 14.6】设 T_d 为任意正常簇头节点从收到第一个判定发起请求到该簇头节点产生测试请求所需的时间上限，T_p 是广播一个分发消息所需的时间上限。对传感节点判定

时间复杂度为 $O(\Delta(T_d+T_p)+T_{out})$，Δ 是图 G 的直径。

证明：在 ΔT_d 时间内，所有的正常簇头节点都会产生测试请求，测试请求产生后，任意正常簇头节点都能在 T_{out} 时间之内判定出其簇成员中传感节点的状态，而最后一个包括传感节点在内的判定结果分发消息将在 ΔT_d+T_{out} 时间内产生。同样，任意分发消息都将在 ΔT_P 时间内被所有的正常簇头节点收到。

14.6.4　网络节点判定处理过程

14.6.4.1　网络簇节点判定

网络中传感节点需要获知其他节点的状态时，先发送一个判定发起请求，簇头节点接收到请求后将向本簇内所有节点发送测试请求，如果收到请求的节点是 Sink 节点，则该 Sink 节点还需向所有簇头节点发送判定发起请求，相邻簇头节点接收到这个判定发起请求后将在本簇内发起判定，通过这种方式将判定广播整个网络。簇头节点接收到簇内节点发送来的测试应答后，将本簇状态封装成分发消息，并通过簇头节点间的逻辑子网广播到所有簇头节点，同时簇头节点也将收集从其他簇头节点发送来的分发消息，测试应答和分发消息均属于判定消息。当簇头节点获知整个网络中所有节点的状态后，判定处理过程结束。

对于传感节点，当收到来自簇头节点的测试请求后，则向相邻节点发送判定发起请求，所有传感节点都将根据测试请求中的测试任务计算出相应结果，生成测试应答，发送到本簇簇头节点。

14.6.4.2　簇头节点自判定

簇头节点对判定过程的集中控制功能决定了簇头节点的故障将导致判定算法的失效，CBCNFD 算法通过采用簇头节点与 Sink 之间的抽象路径——“虚拟链路”，构成一个由簇头节点、Sink 和虚拟链路组成的逻辑子网，在这个逻辑子网上应用 CBCNFD 算法判定簇头节点的状态。

14.6.5　仿真试验与性能分析

基于网络节点系统判定模型，通过网络仿真软件 ns-2 对 CBCNFD 算法进行了仿真，并与 CBSLFD 算法进行比较。

1. 拓扑固定情况的有效性分析

CBCNFD 算法故障判定的触发是由一个簇到另一个簇，在簇内利用簇头节点的集中控制功能对网络节点进行判定，Sink 可被重复判定，重复判定的次数取决于其同时所处的簇个数。CBSLFD 算法中每个节点都产生分发消息，每个分发消息都通过洪泛的方式全网广播，而 CBCNFD 算法中分发消息只由簇头节点产生，并且只由簇头节点和 Sink 进行广播。

CBCNFD 算法在簇头节点对网络节点进行判定之前，首先在簇头节点之间应用 CB-SLFD 算法互相判定。图 14.10 是网络拓扑不变的情况下 CBCNFD 算法与 CBSLFD 算法的有效性能对比。由于 CBCNFD 算法具有拓扑结构的能量有效性和基于节点簇进行比较的特点，简化了比较指令，节省了网络能量，并提高了实时性。

2. 拓扑改变情况的有效性分析

CBCNFD 算法判定过程中网络拓扑发生变化，则每当簇头节点检测到有状态尚未确

定的网络节点进入本簇,就会触发一个判定期,从而系统开销在判定过程中有所增加,但变化不大。图 14.11 是 CBCNFD 算法在网络拓扑变化和固定情况下自身的性能比较。

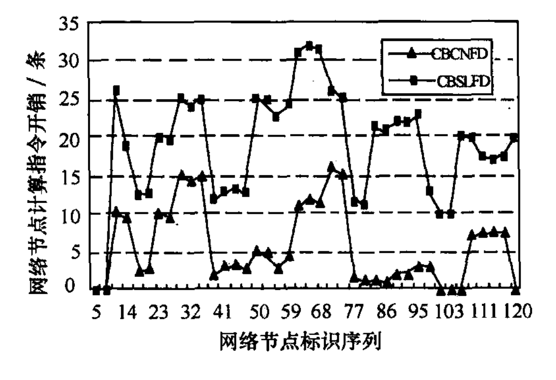


图 14.10　拓扑固定的 CBSLFD 与 CBCNFD 算法对比

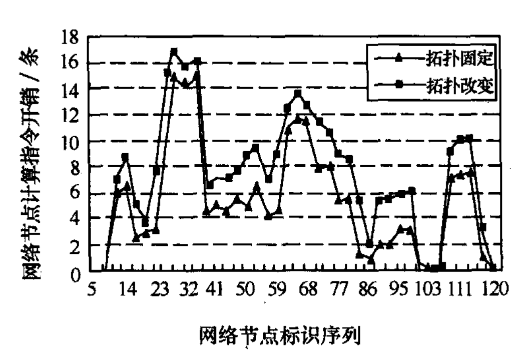


图 14.11　拓扑变化和固定的性能比较

3. 网络规模较大情况的有效性分析

在网络规模较大时,簇头和 Sink 的数量相对于整个网络来说属于少数网络节点。从图 14.12 所示的仿真结果可以看出,CBCNFD 算法总的系统开销远小于 CBSLFD 算法的系统开销,体现了较好的网络能量有效性和网络可扩展性。

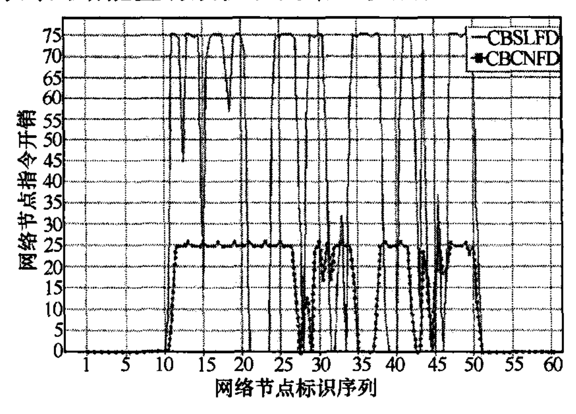


图 14.12　网络规模较大的情况

4. 算法误差分析

预先设定一定数量节点失效,对 CBCNFD 与 CBSLFD 算法进行故障判定的误差比较,如图 14.13 所示。通过多次判定检验,可以看出,CBCNFD 算法绝对误差很小,可有效、准确实现网络节点故障判定,使网络修复具有实时性和高效性。

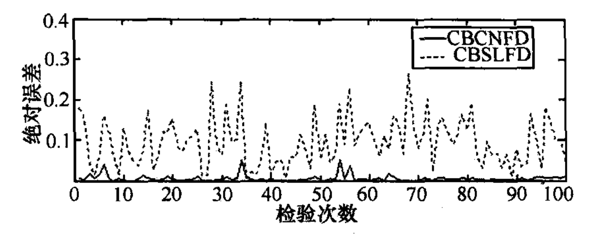


图 14.13　故障判定误差

近年来，国内外针对无线传感器网络提出了许多成簇算法，而无线传感器网络的节点故障判定是成簇算法的必要组成部分。针对节点系统节能、网络能量均衡和网络总体性能要求越来越高的无线传感器网络的应用需求，本文提出的一种新的基于比较的多源网络簇节点故障判定算法，算法优化了判定过程，解决了网络节点的重复判定，减少了系统开销，降低了网络系统能耗，尤其是在网络规模较大，分簇较多的情况下，CBCNFD 算法可以大大降低网络系统的开销，有效延长无线传感器网络生命周期。

参考文献

[1] Karlof C, Sastry N, Shankar U, etc. TinySec: Tinyos Link Layer Security Proposal-version 1.0 [R]. http://webs. cs. berkeley. edu/tos.

[2] Qi X, Ganz A. Runtime Security Composition for Sensor Networks [R]. Multimedia Networks lab ECE department , University of Massachusetts, 2005.

[3] Gruteser M, Schelle G, Jain A, etc. Privacy-aware Location Sensor Networks[C]. In 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), 2003.

[4] Perrig A, Szewczyk R, Wen V. SPINS: Security Protocols for Sensor Networks[C]. In proceeding of the 7th Annual international conference on mobile computing and networks MOBICOM 2001, July 2001: 189 - 199.

[5] Perrig A, Canetti R, Tygar J, etc. Efficient Authentication and Signing for Multicast[C]. In proceeding of NDSS, 2001: 146 - 149.

[6] Perrig A, Tygar J D, Secure Broadcast Communication in Wired and Wireless Networks[M]. Kluwer Academic publisher, 2003: 140 - 148.

[7] Menezes A J, Oorschot P C V, Vanstone S A. Handbook of Applied Cryptography[M]. CRC Press, Boca Raton, FL, 1997.

[8] Perrig A. Canetti R, Tagar D, etc. The TESLA broadcast authentication protocol[R]. Technical report 2, RSA laboratories, 2002.

[9] Anderson R, Bergadano F, Crispo B. A New Family of Authentication Protocols [J]. ACM Operating Systems Review, 1998.

[10] Mitchell C. Romote User Authentication Using Public Information[J]. Cryptography and Coding, 2003.

[11] Bocheng Lai, Sungha Kim, IngrID Verbauwhede. Scalable Session Key Construction Protocol for Wireless Sensor Networks. [C] IEEE workshop on large scale real-time and embedded systems, Austin, Texas, 2002.

[12] Sanchez D, Baldus H. Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks[C]. Proc. Of the First International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005: 277 - 288.

[13] Laurent Eschenauer, Gliger, Virgil D. A Key-management Scheme for Distributed Sensor Networks[C]. Proceeding of the 9th ACM Conference on Computer and Communication Security, 2002: 41 - 47.

[14] Liu D, Ning P. Location-based Pair Wise Key Establishments for Static Sensor Networks[C]. In Proceeding of 1st ACM Workshop on Security of Ad hoc and Security of Ad hoc and Sensor networks. USA, ACM, 2003: 72 - 82.

[15] Huang D, Mehta M, Medhi D, etc. Location-aware Key Management Scheme for Wireless Microsensor Networks[C]. In Proceeding of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks. USA, ACM, 2004: 29 - 42.

[16] Chan H, Perrig A. PIKE: Peer Intermediaries for Key Establishment in sensor Networks[C]. In Proceeding of the IEEE NFOCOM 2005. Piscataway, USA: IEEE, 2005: 524 - 535.

[17] Chan H W, Perrig A, Song D. Random Key Predistribution Schemes for Sensor Networks[C]. Proc 2003 IEEE Symp on Security and Privacy, 2003.

[18] Ross Anderon, Alrian Peerig. Key Infection: Smart Trust for Smart Dust[R]. unpublished Manuscript, 2001.

[19] Du WL, Deng J, etc. A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks[C]. In Proceeding of 10th ACM Conference on Computer and Communications Security, Washington, DC, 2003:42 - 51.

[20] Blom R. An Optimal Class of Symmetric Key Generation Systems[C]. Proceedings of EUROCRYPT' 84. 1984: 335 - 338.

[21] NIST. Advanced Encryption Standard(AES) Development Effort[EB/OL]. http://csrc.nist.gov/2003.

[22] Jolly G, etc. A Low-Energy Key Management Protocol for Wireless Sensor Networks[C]. Proceedings of the 8th IEEE Symposium on Computer and Communications(ISCC223), Antalya, Tureky, 2003.

[23] Carman D, Kruus P, Matt B. Constraints and Approaches for Distributed Sensor Networks Security[R]. Tech, Rep. 00010, NAI Labs, 2000.

[24] Anderson J P. Computer Security Threat Monitoring and Surveillance[R]. Technical report, James P. Anderson Co., Fort Washington, Pennsylvania, 1980.

[25] Denning D E. An Intrusion Detection Model[J]. IEEE Transaction on Software Engineering, 1987, 13(2):222 - 232.

[26] Agah A, Das S K, Basu K. A Game theory based approach for security in wireless sensor networks[C]. In proceeding of international performance computing and communications conference (IPCCC), April 2004:280 - 286.

[27] Agah A, Das S K, Basu K. A Non-cooperative Game Approach for Intrusion in Sensor Network[C]. In proceeding of VTC2004, Fall 2004:45 - 51.

[28] Parr R E. Learning for Markov Decision Processes [D], PhD thesis University of California, Berkeley, 1998:66 - 78.

[29] Edith Ngai. Intrusion Detection in Wireless Sensor Networks[M]. Gmu PMeeting Spring, 2005.

[30] Su Chien Chung, Chang Ko Ming, Kuo Yau Hwang. The New Intrusion Prevention and Detection Approaches for Clustering - based Sensor Networks[J]. IEEE Communications Society/WCNC 2005:1927 - 1932.

[31] Chessa S, Santi P. Comparison Based System-Level Fault Diagnosis in Ad - Hoc Networks[C]. Proc. IEEE 20th Symp. on Reliable Distributed Systems, New Orleans, 2001, 10:257 - 266.

[32] Awadia K, Kumar R. Power Control and Clustering in Ad hoc Networks[A]. IEEE Info com 2003[C], San Francisco, 2003.

[33] 张劼，张宗麟. 基于网络的复杂航空系统远程故障自修复自重构信息系统设计[J]. 航空工程与维修，2007,1: 47 - 50.

[34] Jie Zhang, Bo Jing, Yong Sun. Fault Locating Arithmetic for Multi-Source Network Cluster Nodes Based on Comparison, Proceedings of the 7th World Congress on Intelligent Control and Automation June 25 - 27, 2008, Chongqing, China, 7567 - 7571.

[35] CHESSAS. SANTI Crash Faults Identification in Wireless Sensor Networks[J]. Computer Communications. 2002, 25 (14):1273 - 1282.

[36] Maeng J, Malek M. A Comparison Connection Assignment for Self-Diagnosis of Multiprocessor Systems[C]. Proc. FTCS - 11, 1981:173 - 175.

第 5 篇

无线传感器原型系统与应用实例

第 15 章　无线传感器网络节点平台开发实例
第 16 章　无线传感器网络原型验证系统
第 17 章　无线传感器网络模拟器
第 18 章　无线传感器网络应用实例

第 15 章　无线传感器网络节点平台开发实例

本章以网络能量有效为原则，以“模块化、小体积、低功耗、低成本和通用性”为目标，开发设计嵌入式网络节点硬、软件系统，使其满足监测任务需求的数据采集、计算、无线通信和以太网互联能力。硬件部分主要开发无线通信、微控制器和以太网通信模块，其中，以保证通信效率和通信质量为目标，重点设计微带环形天线和鞭状天线。软件部分设计基于 μC/OS - II 的嵌入式操作系统及相应的接口函数。在硬、软件设计过程中，充分考虑了高频电磁兼容性问题。此外，还研究了 Sink 节点的以太网供电模型。

15.1　网络节点低功耗设计策略[1,2]

15.1.1　微控制器模块低功耗设计

微控制器模块是网络节点的计算中心，选择合适的微控制器在节点设计中至关重要。微控制器功耗主要由工作电压、运行时钟、内部逻辑复杂度以及制作工艺决定，目前，使用电池供电的网络节点，满负荷工作只能持续十几个小时，为了获取更长的生命周期，系统需要在绝大多数时间内处在待机或者休眠状态，但这样限制了无线传感器网络面向应用的优势和以数据为中心的网络特点。

微控制器模块的设计主要考虑以下几个方面：

(1) 选择“够用就好”带 Flash 的 8 位或 16 位简单内核的微控制器，带 Flash 的微控制器可将功耗降低 5 倍。综合考虑数据采集效率与便捷性、处理速度较快、电磁兼容性较强、工作频率较低、信号斜率较慢，稳定性好及应用软件使用 E^2PROM 和片内 Flash 资源的功能需求。本章介绍的网络节点平台中，传感节点采用 MCS - 51 核的 ADμC834，Sink 节点采用 ARM 核的 LPC2210。ADμC834 是采用片上系统(System on Chip, SoC)的高性能微控制器，外围电路简单、运行速度快、有足够的外部通用 I/O 端口和通信接口，并且能够为安全储存和安全通信的软件算法提供必要的硬件支持，芯片尺寸为 15mm × 15mm。LPC2210 是基于一个支持实时仿真和嵌入跟踪的高效 16/32 位 ARM7 TDMI - S 精简指令集 CPU，具有极低的功耗，可确保任务短时间、快速执行。对代码规模有严格控制的应用，通过使用 16 位 Thumb 模式，可将代码规模降低 30%，而性能损失却很小。

(2) 低电压供电可以大大降低系统的工作电流，基于漏电流的考虑，选择 3V(3.3V) 要比 5V 供电的功耗至少降低 40%，本章设计的节点平台采用 3.0V ~ 3.3V 供电。

(3) 由于微控制器内部的运行电流与时钟频率成严格的线性关系，因此综合考虑晶振频率与系统运行速度，尽量降低系统总线频率，并采用锁相环或外部晶振的时钟方案，晶振分别选择 11.0592MHz 和 32.768kHz。

(4) 由于 ADμC834 和 LPC2210 都有快速有效的查表指令和寻址方式，将一些运算结

果预先算好,放在 Flash 或 E^2PROM 中,用查表法替代实时计算,以减少微控制器的运算量,并依据应用设置实时计算精度,避免过度计算,此外使用短的数据类型也是有效的方法。

(5)不用的 I/O 模块或间歇使用的 I/O 模块要及时关掉。

15.1.2　无线通信低功耗设计

无线通信模块是节点系统的重要组成部分,其设计目标是保证通信任务基础上,实现低功耗。

(1)选择合适的 RF 芯片,设计内部损耗低的原理电路和 PCB 电路。

(2)充分考虑硬、软件的电磁兼容性,以提高通信模块的稳定性与可靠性。

(3)设计合理的无线通信机制,提高对无线收发系统能耗的利用与管理。

15.1.2.1　无线收发能耗模型

节点能耗主要由计算能耗、无线通信能耗和传感能耗三部分组成。从 Deborah Estrin 描述的图 3.2 所示的一种传感节点主要模块能量消耗情况中可以看出[3],节点的绝大部分能量消耗在无线通信的收发状态上。收发数据所消耗的能量主要包括以下几部分:

(1)启动收发所需的能量。

(2)发送、接收过程中的消耗。

此外,也有研究表明,传感节点传输 1bit 信息所需要的电能足以执行 3000 条计算指令[4]。

因此,在不影响节点任务功能的前提下,尽可能降低无线通信能耗,成为节点硬、软件设计的核心问题。

简化图 6.10 得到图 15.1 的节点能耗模型。节点将一个数据帧传输至 x_e 处的能耗为 $l_e+\mu_e x_e^{k_e}$。其中,l_e 为传输电路能耗,$\mu_e x_e^{k_e}$ 为射频放大器补偿通道衰减能耗。通道衰减系数 k_e 的取值与节点所处监测区域的环境有关,有障碍物遮挡时 k_e 取 2~5,一般情况下取 3[5,6]。节点接收一个数据帧时,只有接收电路处于工作状态,能耗亦为 l_e。因此,在 x_e 距离内中继一个数据帧的总能耗为 $2l_e+\mu_e x_e^{k_e}$。

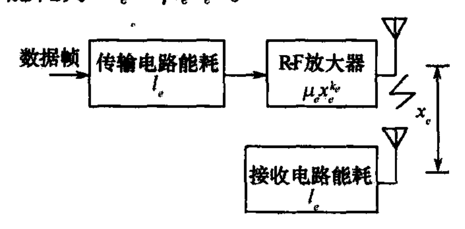


图 15.1　节点无线收发能耗模型

15.1.2.2　无线通信芯片选择

根据节点能耗模型,网络节点的无线通信模块和天线是本章研究与设计的重点内容。目前,在无线传感器网络中应用最多的是射频芯片和 Zigbee 芯片,本设计选用 nRF905 射频芯片完成无线通信[7]。

nRF905 是一个单片 UHF 多段无线收发芯片,其涉足的 433/868/915MHz 频段,信息量较少,可经济实用地实现无线通信;其外设所带来的干扰少、功耗低、成本低,稳定性与

可靠性是其技术亮点；而无线传输无需用户对数据进行曼彻斯特编码，编码由片内硬件自动完成的技术创新非常适合网络节点能量有效性需求，编程和应用非常方便，表 15.1 为 nRF905 射频芯片的主要指标。

表 15.1　nRF905 主要指标

频段/MHz	433(10 个)/868(7 个)/915(169 个)	接收灵敏度/dBm	-105
调制方式	GFSK	数据速率/Kb/s	100
电源电压/V	1.9~3.6	启动时间/ms	3
发射电流/mA	30/10dBm	外围元件数目	20
接收电流/mA	12.5	尺寸/mm	5×5
睡眠电流/μA	2.5	接收灵敏度/dBm	-105

15.1.2.3　无线通信管理的节能机制

由于无线通信占了整个无线传感器网络能耗主要部分，因此，对无线收发系统的能耗管理非常重要，通过采取以下措施可有效减少通信模块的能量损耗：

(1)减少通信流量。减少通信流量的方法包括避免两帧重叠同时发送；增加错误检测和校正机制，以便尽早发现和校正少量错误的数据帧；对传感节点采集的原始数据进行本地计算和簇头节点的数据融合；减少控制帧的开销和帧头长度。

(2)增加休眠时间。由图 3.3 和表 15.1 可知，不需要通信时，尽快使通信模块关闭，进入休眠状态是网络协议设计需要重点考虑的问题。

(3)使用多跳短距离通信方式。无线收发参数 k 的取值与很多因素有关，如部署环境、无线信道质量等，因此在满足通信速率的前提下，尽量减少单跳通信距离，经验而言，通信半径在 100m 内比较合适。

(4)采用功率控制机制。通过调整发送节点的信号发射功率，在保证通信质量的前提下尽量降低信号发射功率，这样既节省了能量，又可降低本节点对其他节点的干扰(多跳网络中同时通信的两对节点都视对方为干扰)，使网络吞吐率得到有效提高。

15.2　传感器节点模块设计

为了使网络节点具有一定的通用性和可扩展性，本节网络节点采用功能模块的板级化设计思想，分别将微控制器模块、无线通信模块、以太网通信模块和数据采集模块单独成板。依据传感节点在网络中的任务与功能需求，设计了如图 15.2 所示的节点功能结构，它由微控制器、传感器与数据采集、无线通信、电源及程序烧写模块组成。

15.2.1　微处理器模块设计

微控制器模块分为采样调理、数据处理、数据存储、通信接口和电源几部分，所有的控制、任务调度、能量计算、功能协调、通信协议、数据整合和数据存储都在微控制器模块支持下完成，包括以下几部分：

(1)模拟信号调理、滤波、放大、A/D 转换。

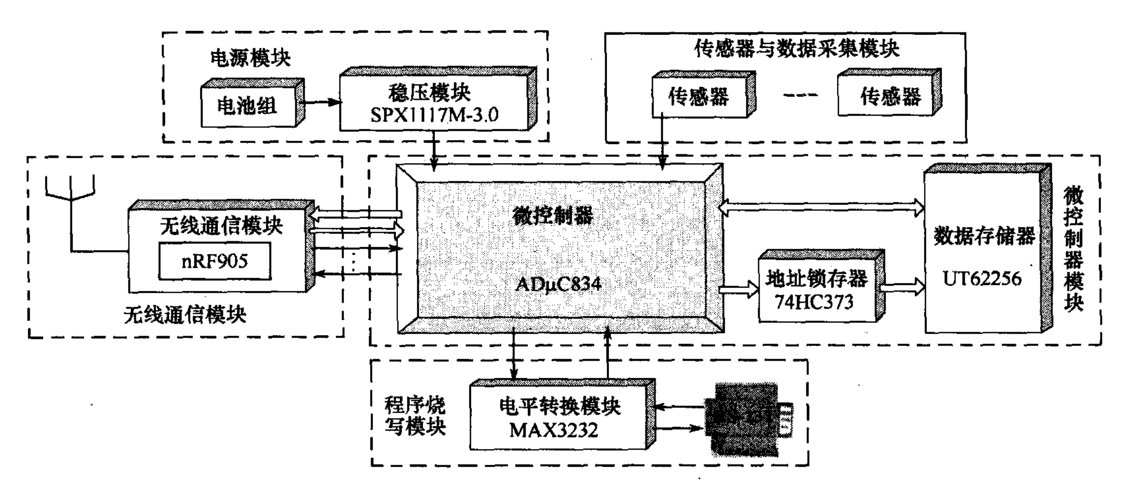


图 15.2　传感节点功能结构

(2)数字信号暂存于缓存中,并对传感器采集的数据进行软件预处理。

(3)提供相应的接口与 RF 模块进行数据交换,负责链路管理与控制、执行基带通信协议和相关的处理过程,包括链接建立、频率选择、链路类型支持和媒体接入控制等。

ADμC834 的 SPI 串行接口数据线与 nRF905 的数据线连接。考虑到 ADμC834 与 nRF905 的通信接口设置,将 P1.1、P1.5、P1.7 接口用于 nRF905 的状态输出控制接口,P1.0、P1.3、P1.4、P1.6 接口用于模拟量数据采集。数字量数据采集直接通过 ADμC834 的 I/O 接口实现,微控制器模块电路原理图如图 15.3 所示。

传感节点工作时,为了减少系统所消耗的电源,可依据任务需求,选择性地关掉系统的某一部分,并且由于 ADμC834 具有 300ms 的快速启动时间(从掉电到工作的恢复时间为 20μs),从而通过延长待机时间,降低电池的使用功耗。

15.2.2　无线通信模块设计

Nordic 的 RF 芯片已经投入实用了,如 2001 新款奔驰轿车的安全系统就采用了 Nordic 的 RF 芯片。Nordic 芯片的特点:Nordic 的传输量在 100Kb/s 以内;外设少是 Nordic 的技术亮点,这样成本低、干扰少、功耗低,保证了产品的技术稳定性;Nordic 的无线传输不需曼彻斯特编码,可直接用最常用的串口来进行,这样对编程和应用非常方便。曼彻斯特编码效率低,容易出错,采用曼彻斯特编码的芯片在编程上会需要较高的技巧和经验,需要更多的内存和程序容量,其他无线收发芯片由于技术的原因都需要这种技术来传输,而 Nordic 有这方面的技术创新也非常适合本文设计的无线传感器网络节点。因此,本文选用 nRF905 芯片来完成无线通信。

在 Nordic 目前涉足的 433/868/915MHz 频段,信息量较少;可传输几十米、甚至数百米,因此普通 nRF905 可实用经济地实现无线通信。它只需要非常少的外部元件,体积小,可以满足无线传感器节点硬件集成的需求,由于所需的外围器件很少,所以易于调试和编程。nRF905 芯片一般在 3 美元以下,成本较低。

无线通信模块是网络节点的重要组成部分,需要满足低功耗、通信质量、通信距离、通

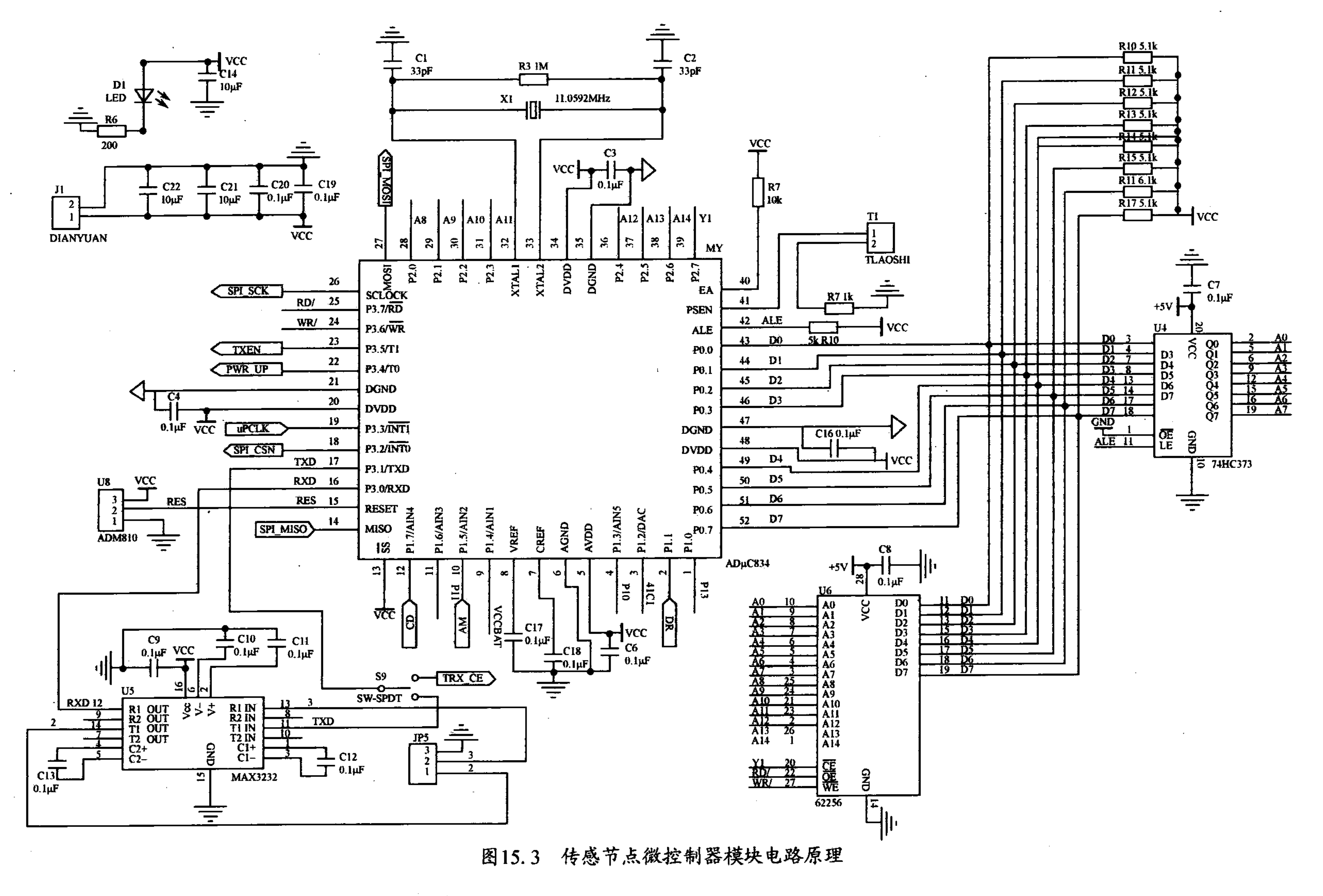


图15.3 传感节点微控制器模块电路原理

信速度、组网方便、抗干扰和易于布控等要求。

由于 nRF905 采用了优化的高斯频移键控(Gaussian frequency shift keying, GFSK)调制解调技术,抗干扰能力较强,提高了数字通信频谱利用率和通信质量。nRF905 片内集成了电源管理、晶体振荡器、低噪声放大器、频率合成器、功率放大器等模块,不用外加声表面振荡器,曼彻斯特编码/解码由片内硬件完成。由于采用了自动增益控制技术,能根据调节信号的强弱自动调节比较电路门限。nRF905 用户接口、工作模式切换时序、操作模式与编程设置详见文献[7]。

图 15.4 是无线通信模块电路原理图,nRF905 通过 SPI 接口与 ADμC834 进行数据交换,主要包括射频和基带两部分,前者提供数据通信的空中接口(Air Interface),也称无线接入技术,后者提供链路的物理信道和数据分组。状态输出接口均接 ADμC834 I/O 接口,该电路自动完成数据封装成帧(加字头和 CRC 校验码)与发送,在接收中有载波检测和地址匹配检测引脚,接收到正确的数据帧时,自动移去字头、地址和 CRC 校验码,然后通知 ADμC834 读取数据。

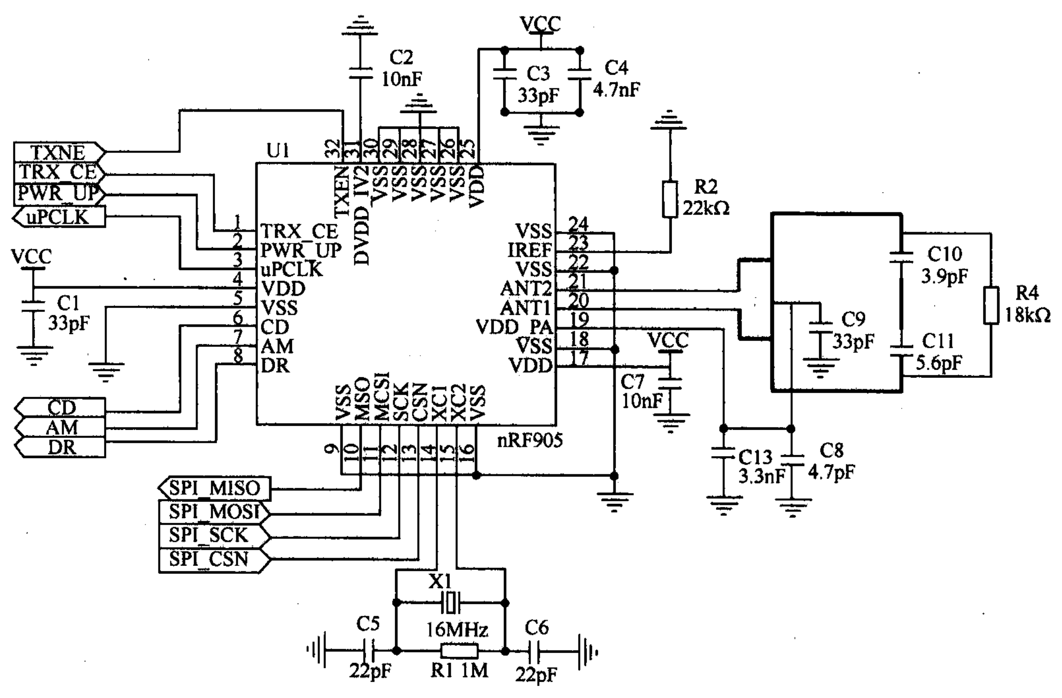


图 15.4 无线通信模块电路原理图

鞭状天线电路原理如图 15.5 所示,图 15.6 分别为 PCB 天线与鞭状天线实物图。

天线的效率一般都随工作频率的提高而增加,当天线的有效长度接近其工作频率半波(1/2 波长)的正整数倍时,天线的效率较高。若这个倍数增加时,天线的效率还会进一步提高。

15.2.3 传感节点软件设计

传感节点系统的软件部分采用模块化结构,各功能模块均编成子程序,便于软件系统的调试和完善。传感节点的这部分程序主要分为主程序、数据采集与数字滤波子程序、

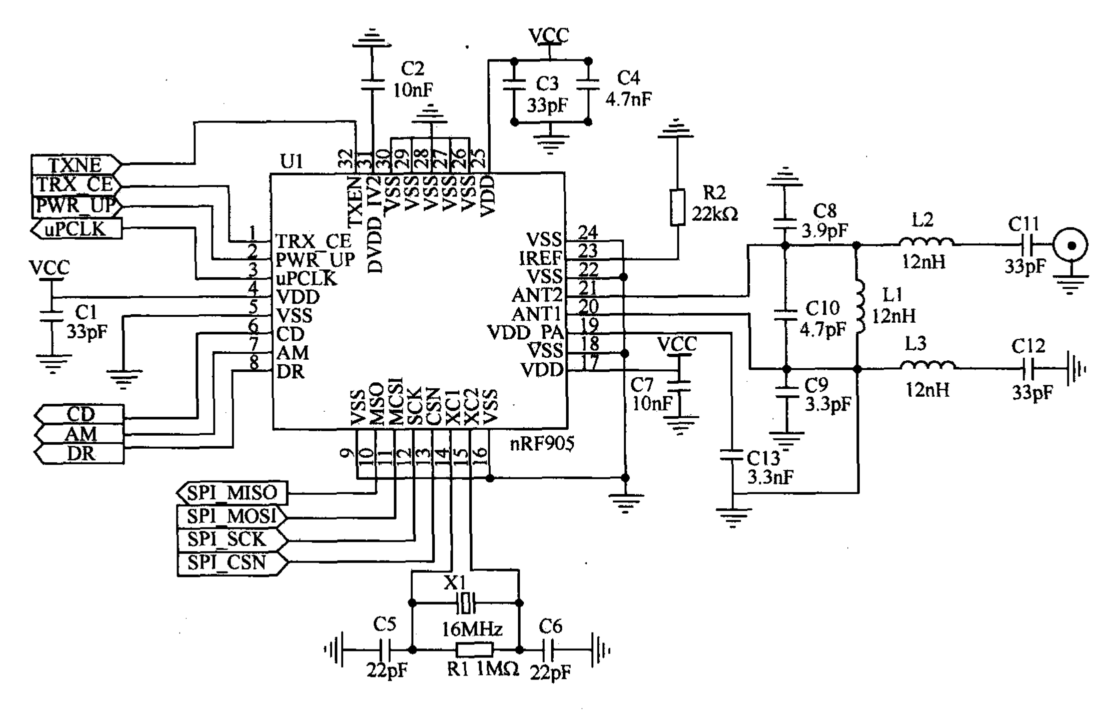
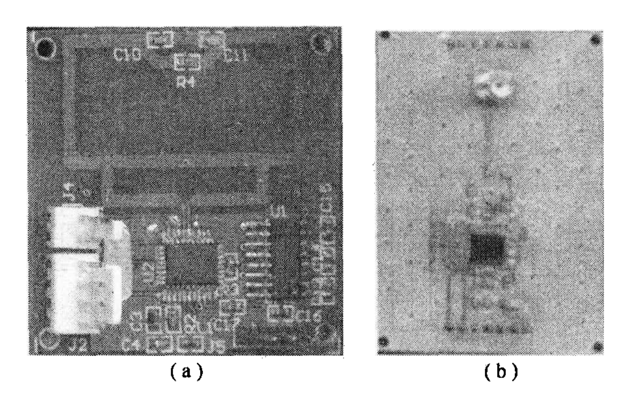


图 15.5　鞭状天线原理图



(a)　　(b)

图 15.6　微带天线与鞭状天线实物图

A/D 通道转换子程序、看门狗监控子程序、通信模块配置子程序和通信模块低功耗配置程序。限于篇幅和实现的难易程度，本节主要阐述主程序、A/D 通道转换子程序、通信模块配置子程序和通信模块低功耗配置程序。

15.2.3.1　主程序设计

在本系统中，ADμC834 作为一个智能采集模块，其主要功能是采集并存储信号，并根据簇头节点的命令完成无线数据传输的操作。主程序是整个程序框架的主体，所有的子程序均由主程序调配使用，完成数据采集、传输、发送、接收和各种命令的处理。整个程序分为命令处理、ADC 处理和通信处理三大模块。处理器模块的主程序流程如图 15.7 所示。数据采集与数字滤波采用移动式算术平均法，子程序流程图如图 15.8 所示。

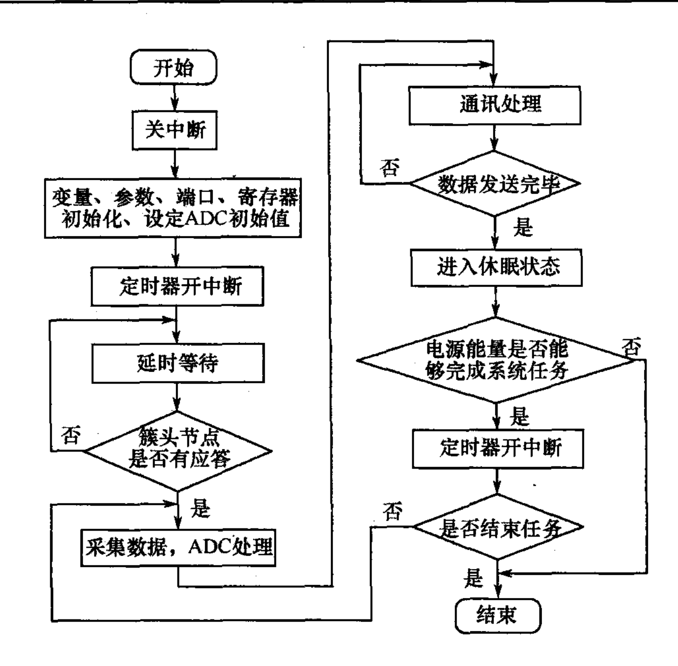


图 15.7　处理器模块的主程序流程

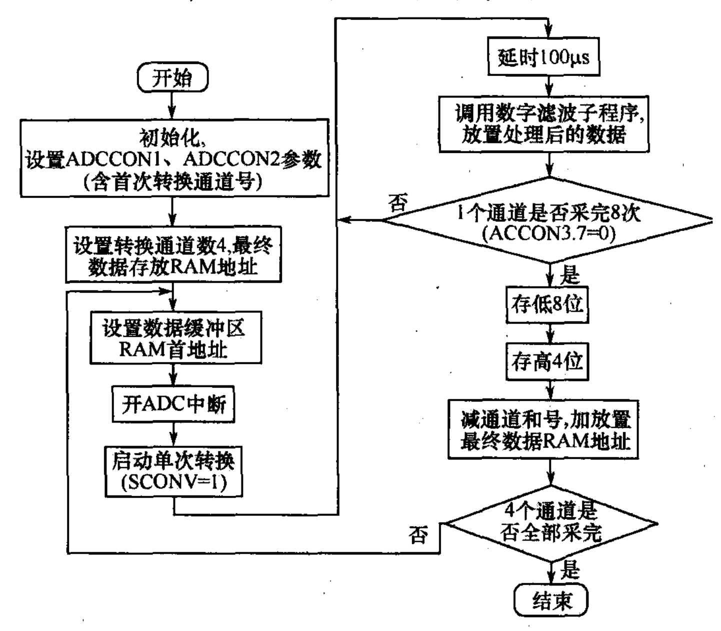


图 15.8　数据采集与数字滤波子程序

15.2.3.2　A/D 通道转换配置子程序

一个传感节点带有 5 路 A/D 接口，可同时采集 5 路数据，源程序如下：

```
#include <ADμC834.H>
#include <stdio.h>
void main (void)
{
unsigned char chan_2_convert;
/*-------------------------配置串口,波特率 9600 ------------------------*/
```

```
        SCON  = 0x50;                    //SCON:模式1,8 位 UART;
        TMOD  = 0x20;                    //TMOD:定时器1,模式2;
        TH1  = 0xFD;                     //TH1:加载 9600 baud @ 11MHz;
        PCON & = 0x7F;                   //SMOD:重置 SMOD 位,倍频;
        TR1  = 1;                        //TR1:定时器1运行;
        TI  = 1;                         //TI:放置 TI 为 UART 第一个变量;
        EA  = 1;
/* ------------------------------配置 A/D,切换输入通道------------------------------* /
ADCCON1  = 0xFC;              //1111 1100
while (1)
        {
        unsigned int conv_val;
        unsigned char channel;
/* ------------------------------配置开始,等待配置完成------------------------------* /
        chan_2_convert  = (chan_2_convert + 1) % 8;
        ADCCON2  = (ADCCON2 & 0xF0) |chan_2_convert;
        SCONV  = 1;
        while (ADCCON3 & 0x80);
/* ------------------------------读 A/D 数据,并送出------------------------------* /
   channel  = ADCDATAH > > 4;
        conv_val  = ADCDATAL |((ADCDATAH & 0x0F) < < 8);
        printf ("ADC Channel % bu  = 0x% 4.4X\r\n", channel, conv_val);
        }
}
```

在本设计中,考虑到 MCU 与通信模块的通信接口设置,将 P1.1、P1.5、P1.7 接口用于 nRF905 的状态输出控制接口,P1.0、P1.3、P1.4、P1.61 接口用于模拟量数据采集,数字量数据采集直接通过 ADμC834 的 I/O 接口实现。

15.2.3.3　无线通信功能模块配置与低功耗模式配置子程序设计

nRF905 所有配置都通过 SPI 接口进行。SPI 接口由 5 个内部寄存器组成,执行寄存器的回读模式来确认寄存器的内容,如图 15.9 所示。SPI 指令用来决定进行什么操作,SPI 接口只有在掉电模式和 Standby 模式是激活的。

nRF905 初始化流程如图 15.10,其主要功能包括对状态寄存器、射频配置寄存器、地址寄存器、发送数据寄存器、接收数据寄存器进行合理的配置。

(1)状态寄存器(Status – Register)。包含数据就绪(DR)和地址匹配(AM)状态。

(2)RF 配置寄存器(RF – Configuration Register)。包含收发器的频率,输出功率等配置信息。

(3)发送地址(TX – Address)寄存器。包含目标地址,字节长度由配置寄存器设置。

(4)发送有效地址(TX – Payload)寄存器。包含发送的有效 ShockBurst 数据包数据,字节长度由配置寄存器设置。

(5)接收有效数据(TX – Payload)寄存器。包含接收到的有效 ShockBurst 数据包数据,字节长度由配置寄存器设置。在寄存器中的有效数据由数据准备就绪指示。

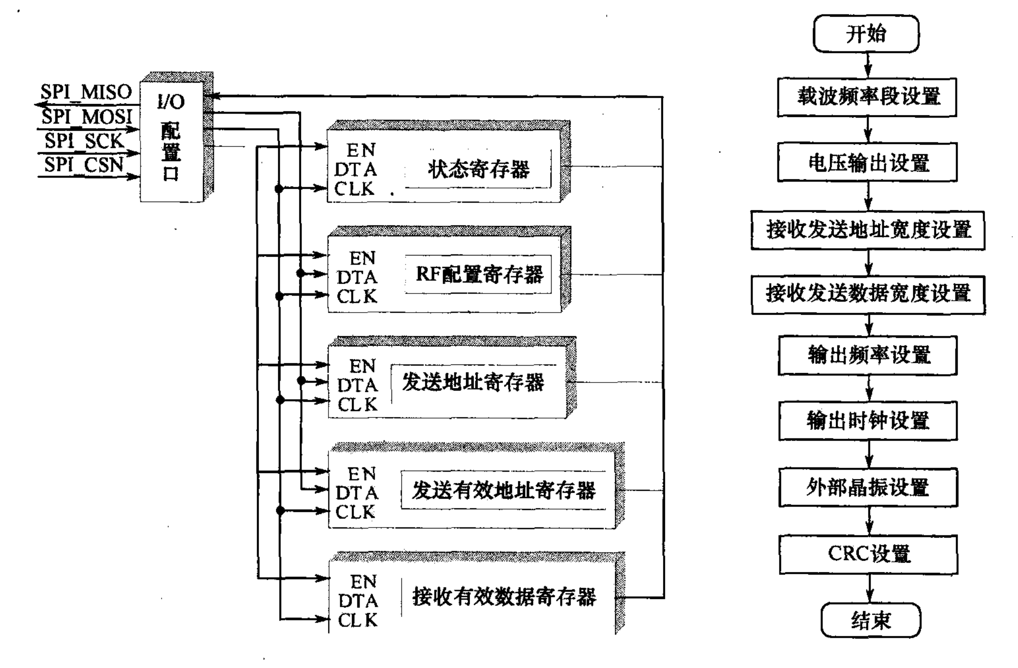


图 15.9　nRF905 内部寄存器

图 15.10　nRF905 初始化流程图

nRF905 有两种工作模式,分别为 ShockBurst™接收模式和 ShockBurst™发送模式。

(1)nRF905 发送流程。当微控制器有数据要发送时,通过 SPI 接口,按时序把接收机的地址和要发送的数据传给 nRF905,SPI 接口的速率在通信协议和器件配置时确定;微控制器置高 TRX_CE 和 TX_EN,激发 nRF905 的 ShockBurst™发送模式;当数据发送完成,数据准备好(DR)引脚被置高;AUTO_ RETRAN 被置高,nRF905 不断重发,直到 TRX_CE 被置低;当 TRX_CE 被置低,nRF905 发送过程完成,自动进入空闲模式。

(2)nRF905 接收流程。TRX_CE 为高、TX_EN 为低时,nRF905 进入 ShockBurst™接收模式。当一个正确的数据包接收完毕,nRF905 自动移去字头、地址和 CRC 校验位,然后把数据准备好引脚置高,微控制器把 TRX_CE 置低,nRF905 进入空闲模式。

对于 SPI 指令设置,当 CSN 为低时,SPI 接口开始等待一条指令,任何一条新指令均由 CSN 的由高到低的转换开始。nRF905 配置源程序如下:

系统配置文件(OS_CFG. H)

```
OS_CFG. H( )
#define OS_MAX_EVENTS       2  //定义系统中可分配的事件控制块的最大数目,必须大于0
#define OS_MAX_MEM PART     2  //定义系统中内存块的最大数目,必须大于0
#define OS_MAX_QS           2  //定义系统中可以创建的消息队列的最大数目,必须大于0
#define OS_MAX_TASKS        11 //定义用户程序中可以使用的最多任务数,必须大于等于2
#define OS_LOWEST_PRIO      12 //设定系统中要使用的最低任务优先级(最大优先级数),≤63
#define OS_TASK_IDLE_STK_SIZE   512   //设定空闲任务的堆栈容量
#define OS_TASK_STAT_EN         1     //设定系统是否使用统计任务
#define OS_TASK_STAT_STK_SIZE   512   //设置统计任务的堆栈容量
#define OS_CPU_HOOKS_EN         1     //设定是否在 OS_CPU_C.C 中声明对外接口函数
#define OS_MBOX_EN              0     //控制是否使用消息邮箱函数及相关的数据结构
```

```
#define OS_MEM_EN                0    //控制是否使用内存块管理函数及相关的数据结构
#define OS_Q_EN                  0    //控制是否使用消息队列函数及相关的数据结构
#define OS_SE_EN                 1    //控制是否使用信号量管理函数及相关的数据结构
#define OS_TASK_CHANGE_PRIO_EN      0    //控制是否使用 OSTaskChangePrio()函数
#define OS_TASK_CREATE_EN           1    //控制是否使用 OSTaskCreate()函数
#define OS_TASK_CREATE_EXT_EN       0    //控制是否使用 OSTaskCreateExt()函数
#define OS_TASK_DEL_EN              0    //控制是否使用 OSTaskDel()函数
#define OS_TASK_SUSPEND_EN           0    //控制是否使用 OSTaskSnspend()和 OSTa-
                                              skResume()函数
#define OS_TICKS_PER_SEC           64    //设定调用 OS_TimeTick()函数的频率
```

15.2.3.4　无线收发模块数据收发协议设计

无线收发模块分发送和接收两部分,发送功能模块负责数据包的生成和发送。这些功能都是有硬件电路自动实现,软件只是把将要发送的数据用 SPI 总线从微处理器送至发送数据寄存器中和切换至发送工作模式,整个发送数据的流程如图 15.11 所示,功能模块的源程序如下:

```
void nRF905Trans(void)
{
PWR_UP =0;
TRX_CE =0;
DelayXus(8);
PWR_UP =1;
TX_EN =1;
TRX_CE =0;
WirteDataTo905(0x38);
DelayXus(8);
TRX_CE =1;
While(TRX_CE =1) ;
}
```

接收功能模块负责载波信号的检测,地址匹配检测和数据包的解码和接收。这些功能也都由硬件电路自动实现,软件只是将要接收到的数据用 SPI 总线从接收数据寄存器之中送至微处理器,结束后将系统切换至空闲模式。整个接收数据的流程如图 15.12 所示,功能模块的源程序如下:

```
void nRF905Receive(void)
{
PWR_UP =0;
TRX_CE =0;
DelayXus(8);
PWR_UP =1;
TRX_CE =0;
TX_EN =1;
WirteDataToMCU(0x38);
}
```

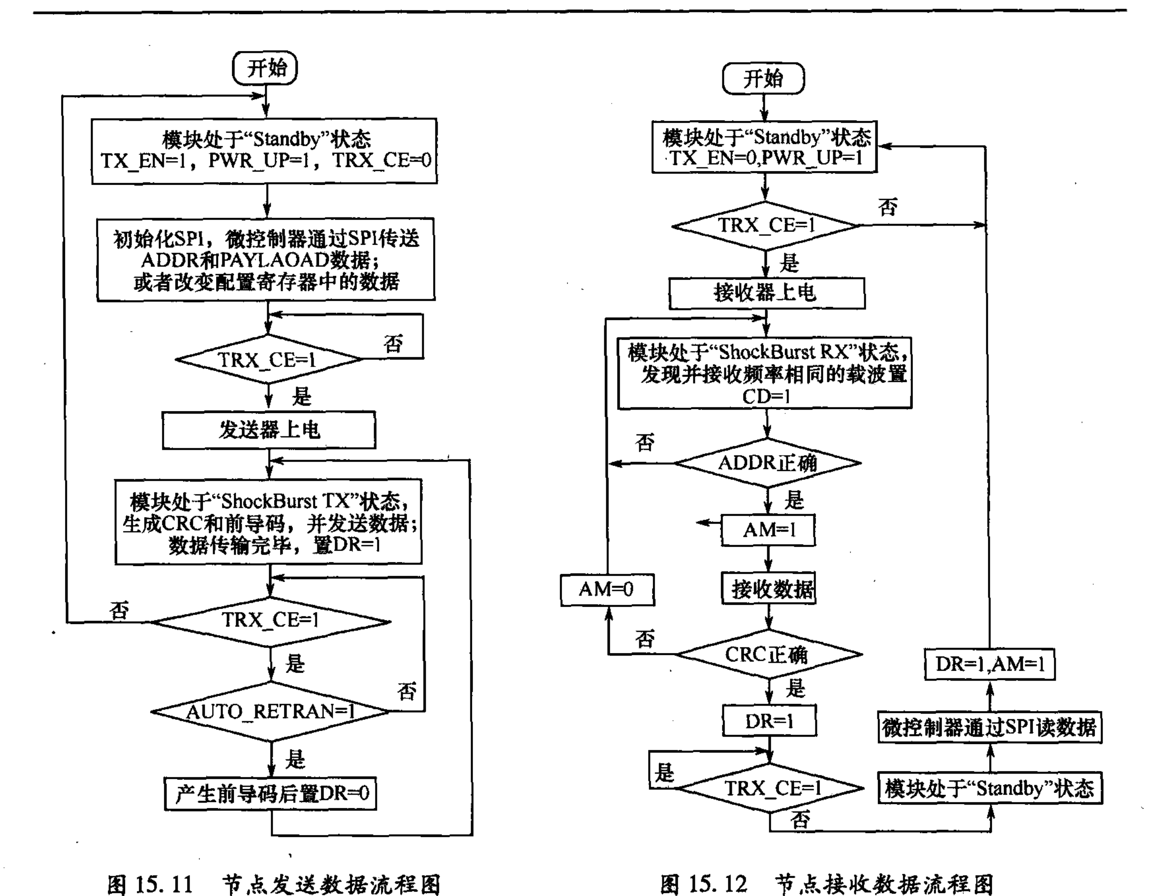


图 15.11　节点发送数据流程图　　　　图 15.12　节点接收数据流程图

上述的发送与接收流程对于传感节点无线数据收发模块、簇头节点无线数据收发模块和 Sink 节点无线数据收发模块三部分都是适用的，流程结构完全一致，所不同的是各个节点的部分语句，传感节点特有的主要语句如下：

```
/* ----------------------传感节点发送工作程序------------------------* /
void Sensor Process ()              //嵌入式传感节点端工作程序
{
  Init905 (1, 0 );                  //nRF905 工作在发射状态,信道 0
  while (1)
    {
      if(Buffer0Tail > =9)          //数据获取完毕
        {
WirelessDataPackaging ();           //将数据打包
WirelessDataSend ();                //无线发送数据;
WirelessBufferClear ();             //无线接收缓冲区清理
}
   }
}
/* ----------------------传感节点接收工作程序--------------------------* /
void Sensor Process()               //嵌入式传感节点端工作程序
```

```
{
Init905 (0, 0);             //905 工作在接收状态,信道 0
while (1)
{
if(GetKeyWord())            //获取匹配关键字,滤掉杂波
if (CheckData())            //获取无线数据并校验
}
}
```

在系统运行过程中,传感节点利用 MCU 串口接收数据,数据采集完毕后,进行数据打包,添加校验位。进入发射状态,将数据发出,然后进入低功耗模式(空闲模式)。

15.3　Sink 节点的特殊性设计

本章设计的 Sink 节点具有 Web 服务器功能,其功能结构如图 15.13 所示。它由微控制器、以太网互联与供电、无线通信、程序烧写调试和性能检测模块组成,通过 RTL8019AS/DM9000 接入以太网,通过 nRF905 无线收发数据。

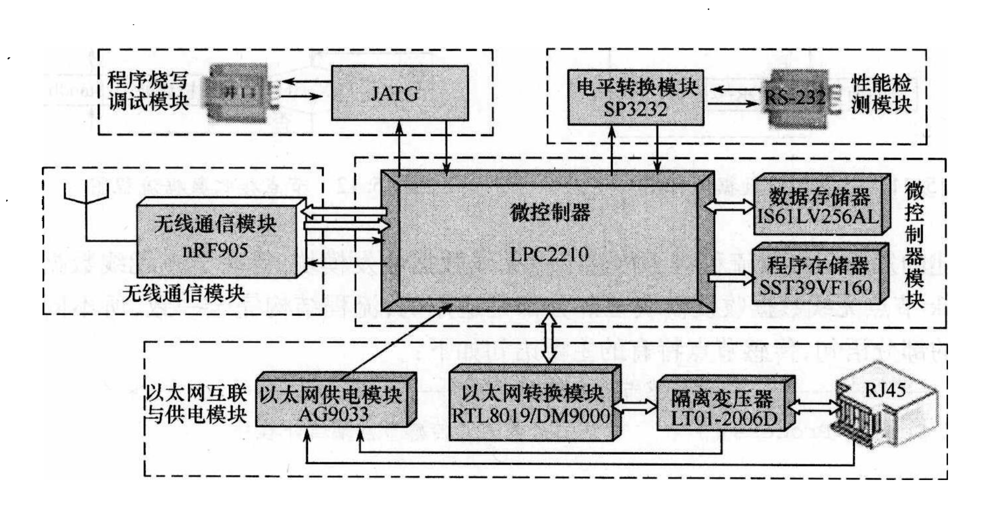


图 15.13　Sink 节点功能结构

15.3.1　处理模块设计

Sink 节点是无线传感器网络中的特殊节点,具有大量内存、外存、高吞吐率和处理能力。Sink 节点负责基站与无线传感器网络的通信及与以太网的互联,故需要一个串口通信模块和一个以太网通信模块。

微控制器模块主要组成: ARM LPC2210、SRAM IS61LV25616AL(256K)、Flash SST39VF160(16M)、串行电平转换芯片 SP3232E、复位芯片 SP708S、硬件接口 11 针无线通信总线接口、电源 AG9033(3.3V)。微控制器模块原理如图 15.14 所示,实物如图 15.15 所示。

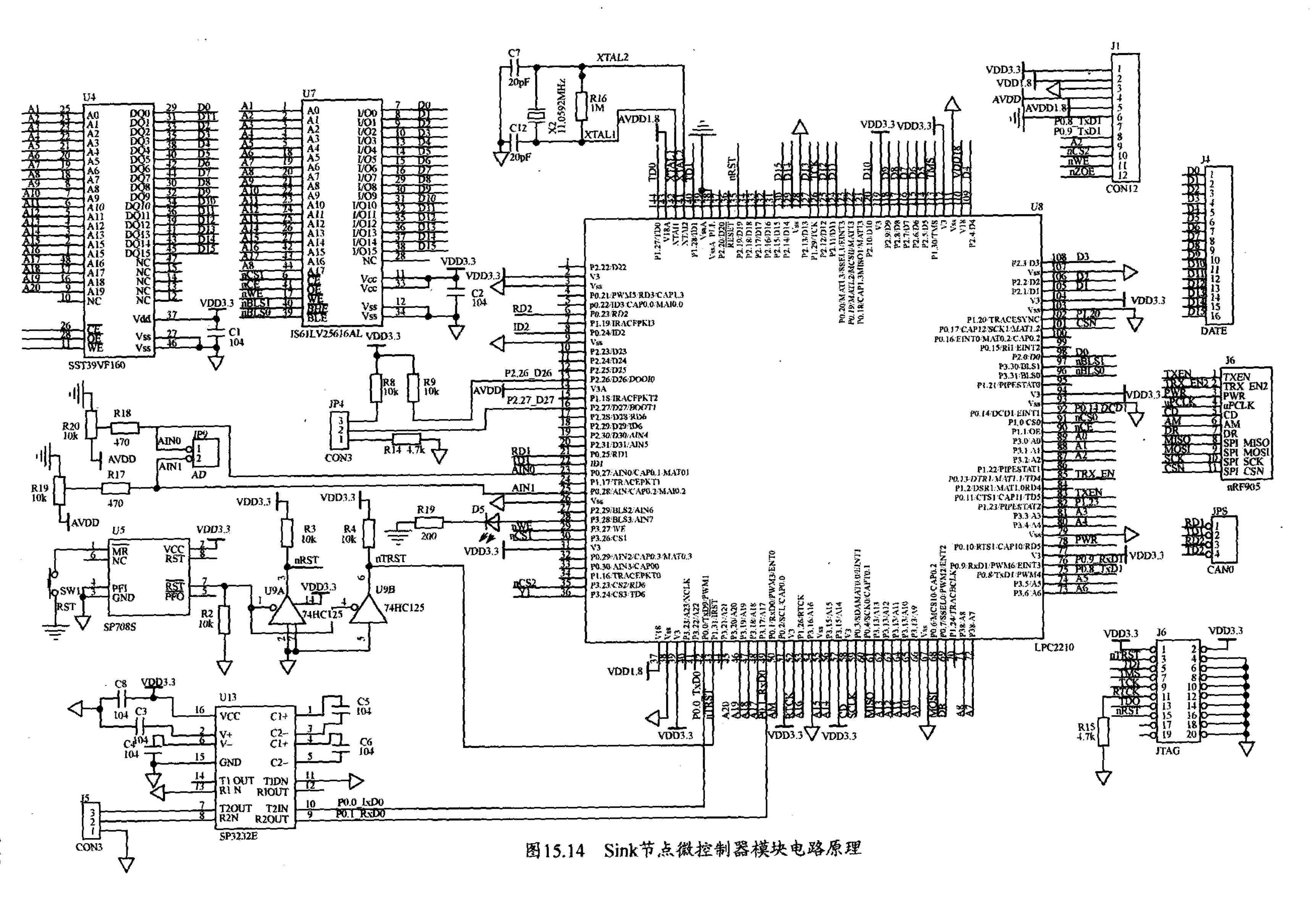


图15.14　Sink节点微控制器模块电路原理

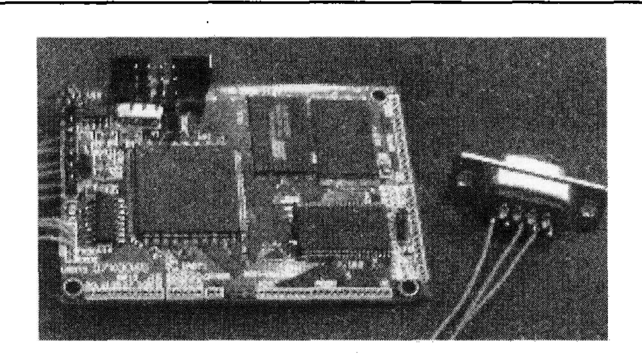


图 15.15　Sink 节点微控制器模块实物图

15.3.2　以太网互联模块设计

以太网是目前 TCP/IP 采用的主要互联网技术,它向上通过 ARP 地址解析协议完成与 IP 协议之间的地址转换,向下采用 CSMA/CD 作为介质访问控制方法。

Sink 节点以太网接入基础层功能由网络接口控制芯片(Network Interface Control, NIC)自动完成。采用为 10Mb/s 网络适配器设计的 RTL8019AS 作为网络接口控制芯片,其好处是 NE2000 兼容、软件移植性好、接口简单和不需转换芯片(如 PCI - ISA 桥),以太网模块电路原理图如图 15.16 所示。

RTL8019AS 具有标准的 ISA 接口,用 LPC2210 控制 RTL8019AS 实现数据发送功能时,需要 16 位数据总线和 20 位地址总线对 RTL8019AS 通信及其内部寄存器进行控制。RTL8019AS 内部寄存器分成 4 页,每页 16 个寄存器,寄存器寻址由以下 3 个因素决定:

(1)命令寄存器中的 PS1 和 PS0 位,决定访问寄存器的哪一页。

(2)4 条地址线 RA0 - RA3,决定访问一页中哪一个寄存器。

(3)读写信号 IOWB/IORB,决定寄存器的读写操作。

此外,由于目前交换机的货架规格、通信方式与网络带宽的不同,还设计了以 DM9000 芯片组成的以太网互联模块,它是 10Mb/s/100Mb/s 自适应全双工通信芯片,具有普适性,基于 DM9000 的以太网模块电路原理图如图 15.17 所示。

15.3.3　无线通信软件设计

15.3.3.1　节点通信程序

Sink 节点与簇头节点、基站主机和远端用户通信流程如图 15.18 所示。Sink 节点进入接收状态后,接收端不断监测信号,判断系统工作的关键字匹配则接收下面的数据,并加以校验判断,无误数据通过 RS - 232C 口传给基站主机,通过 RJ45 口传给远端用户。Sink 节点数据接收和发送流程的部分代码如下:

```
/* ---------------------------------Sink 节点端工作程序---------------------------------* /
void SinkProcess()            //嵌入式 Sink 节点工作程序
{
Init905 (0, 0) ;              //905 工作在接收状态,信道 0
while (1)
{
```

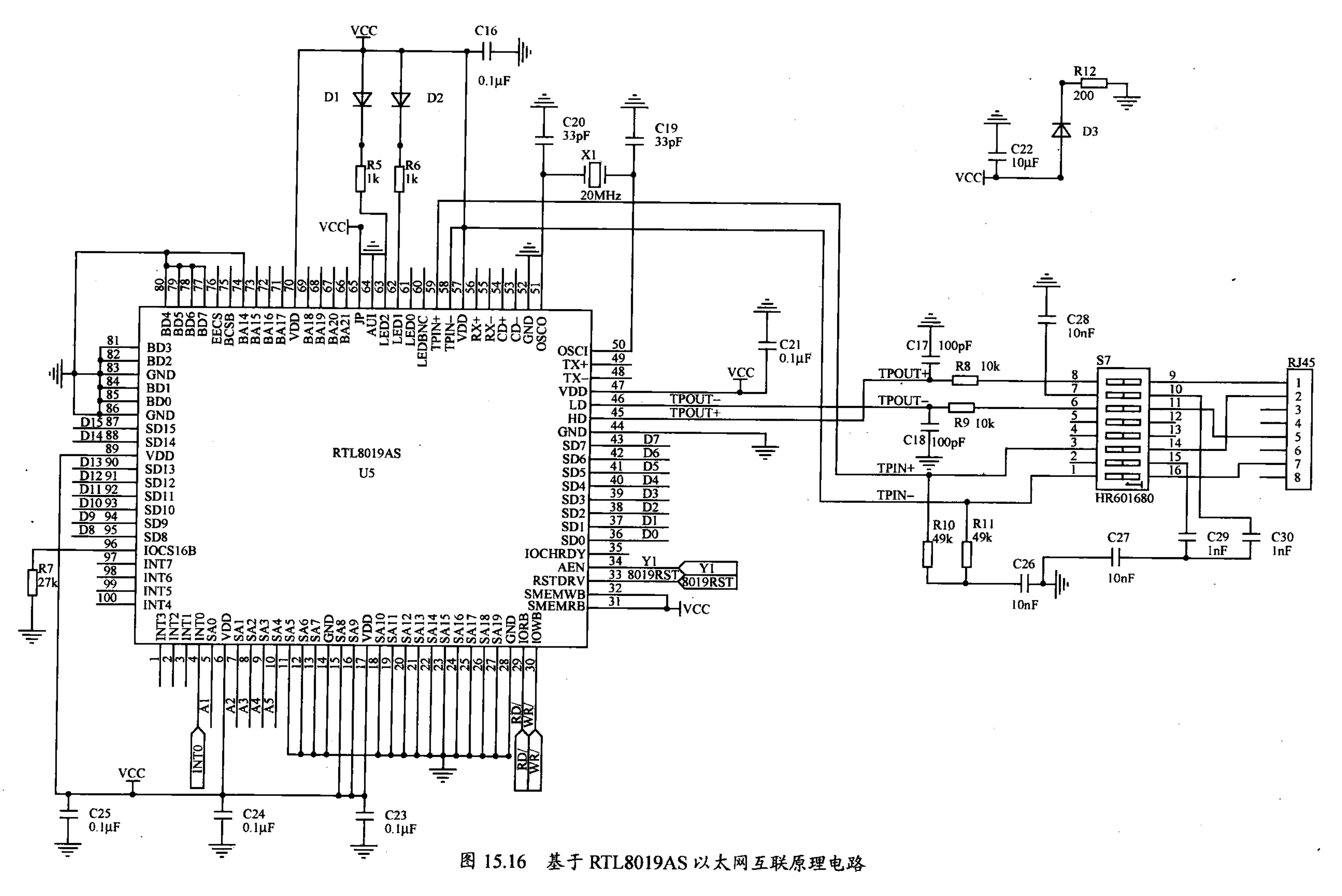


图 15.16　基于 RTL8019AS 以太网互联原理电路

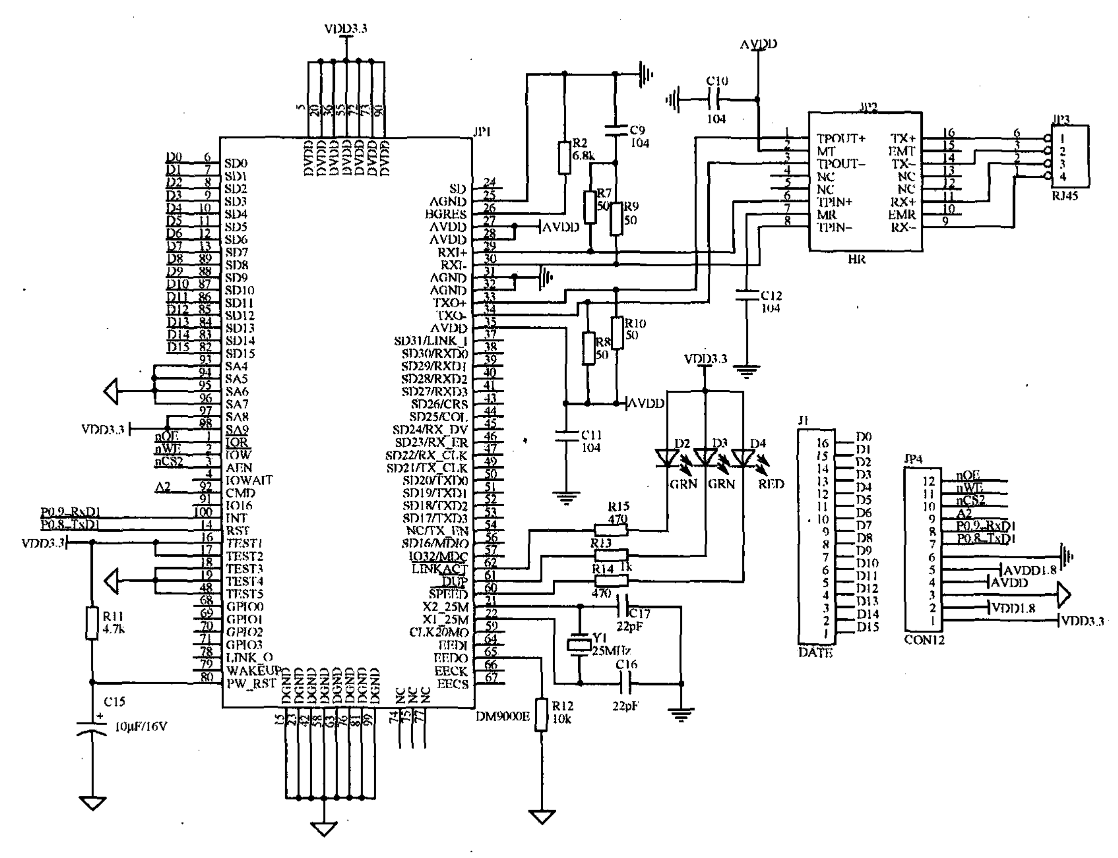


图 15.17　基于 DM9000 以太网互联原理电路

```
if(GetKeyWord())          //获取匹配关键字,滤掉杂波
if (CheckData())          //获取无线数据并校验
    SendDataToPC          //校验通过传递给基站 PC 机
}
}
```

簇头节点与 Sink 节点的接收流程相似,簇头节点进入接收状态后,接收端不断监测空中信号,判断系统工作的关键字 ID 是否匹配,滤掉杂波。关键字 ID 匹配则接收下面的数据,并加以校验判断,数据无误才发送给 Sink 节点,发送完毕进入低功耗模式。簇头节点无线数据收发程序流程如图 15.19 所示。

簇头节点数据接收和发送源程序的主要代码如下:

```
/*---------------------------簇头节点端工作程序---------------------------*/
void ClusterProcess()          //嵌入式簇头节点工作程序
{
Init905 (0, 0);                //905 工作在接收状态,信道 0
while (1)
{
if(GetKeyWord())               //获取匹配关键字,滤掉杂波
if (CheckData())               //获取无线数据并校验
    {
```

```
Init905 (1, 0 );                //nRF905 工作在发射状态,信道 1
SendDataToSink;                 //校验通过传递给 Sink 节点
}
}
}
```

开 始
Sink 节点进入接收状态，延时5ms
簇头节点关键字ID是否与Sink节点匹配？
否
是
Sink 节点接收数据
校验和正确？
否
是
通过内部总线将数据传输至数据处理单元
(1) 通过RS-232发送数据至主控 PC机；
(2) 通过RJ-45发送数据至以太网
发送完毕，通过STBY和PWR_DWN设置，Sink节点系统进入低功耗模式
返 回

图 15.18　Sink 节点通信工作流程

开 始
簇头节点进入接收状态，延时5ms
传感节点关键字ID是否与簇头节点匹配?
否
是
簇头节点接收数据
校验和正确?
否
是
通过内部总线将数据传输至数据处理单元
发送处理后的数据至Sink节点
发送完毕，节点系统进入低功耗模式
返 回

图 15.19　簇头节点无线数据收发程序

15.3.3.2　以太网通信驱动软件设计

RTL8019AS 完成数据帧和电平信号之间的相互转换,物理信道上的收发操作采用以太网协议 802.3 帧格式,以太网驱动程序通过读写 NIC 相关寄存器,控制以太网帧的收发。RTL8019AS 分为本地直接存储器存储 DMA(Direct Memory Access)和远端 DMA 两个功能区。网络接口通过本地 DMA 和远端 DMA 来完成数据的收发。本地 DMA 为 RTL8019AS 内部数据传输,远端 DMA 指 RTL8019AS 与 LPC2210 之间的数据传输,对应关系及部分相关寄存器如图 15.20 所示。本地 DMA 是由 NIC 内部电路自动完成的,远端 DMA(以太网驱动程序)需根据 RTL8019AS 芯片工作机制自行编写,以太网驱动程序分

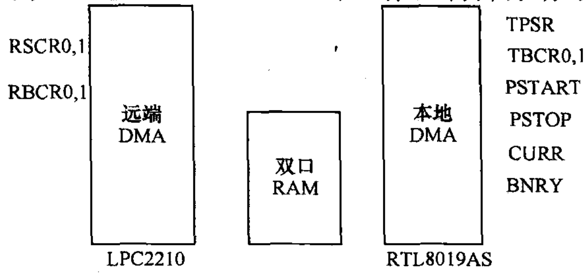


图 15.20　RTL8019AS 数据收发相关寄存器

为 RTL8019AS 芯片初始化、以太网帧接收程序和帧发送程序。

1. 初始化

RTL8019AS 上电复位后，对各寄存器进行初始化、分配数据缓冲区，注册低级中断处理程序、创建发送和接收数据的高级中断处理程序，并启动 RTL8019AS 与 LPC2210 进行交互。源代码如下：

```
void RTL8019dev_init(void)
{
    INT16U COUNT;
    RTL8019setupPorts();
    HARD_RESET_RTL8019();
    writeRTL( ISR, readRTL(ISR) ) ;
    for(COUNT =0;COUNT <15000;COUNT + +);
    writeRTL(CR,0x21);
    for(COUNT =0;COUNT <2000;COUNT + +);
    writeRTL(DCR, DCR_INIT);
    writeRTL(RBCR0,0x00);
    writeRTL(RBCR1,0x00);
    writeRTL(RCR,0x04);
    writeRTL(TPSR, TXSTART_INIT);
    writeRTL(TCR,0x02);
    writeRTL(PSTART, RXSTART_INIT);
    writeRTL(BNRY, RXSTART_INIT);
    writeRTL(PSTOP, RXSTOP_INIT);
    writeRTL(CR, 0x61);
    for(COUNT =0;COUNT <2000;COUNT + +);
    writeRTL(CURR, RXSTART_INIT);
    writeRTL(PAR0 +0, MYMAC_0);
    writeRTL(PAR0 +1, MYMAC_1);
    writeRTL(PAR0 +2, MYMAC_2);
    writeRTL(PAR0 +3, MYMAC_3);
    writeRTL(PAR0 +4, MYMAC_4);
    writeRTL(PAR0 +5, MYMAC_5);
    writeRTL(CR,0x21);
    writeRTL(DCR, DCR_INIT);
    writeRTL(CR,0x22);
    writeRTL(ISR,0xFF);
    writeRTL(IMR, IMR_INIT);
    writeRTL(TCR, TCR_INIT);
    writeRTL(CR, 0x22);
}
```

2. 数据帧接收

数据帧接收分以下两步完成：

(1)由本地 DMA 将数据帧读入接收缓冲环中,并由远端 DMA 将缓冲环中数据读入内存。在本地 DMA 启动之前,应对 PSTART、PSTOP、CURR、BNRY 等寄存器初始化。PSTARY 为接收缓冲环的起始页地址;PSTOP 为接收缓冲环停止页地址,这一页不用来存放数据,CURR 为写缓冲环指针,指向此时要写的页,受芯片控制,BNRY 为读缓冲环指针,指向已经读走的最后一页,由主程序控制。通过"CURR = BNRY + 1?"可以判断出是否收到新数据帧,新收到的数据帧存于 CURR 指出的地址为首址的 RAM 中,当 CURR = BNRY 时,芯片停止接收数据帧。

(2)在启动远端 DMA 之前,需对 RSAR 和 RBCR 等寄存器设置,数据接收程序流程如图 15.21 所示。

3. 数据帧发送

首先,把内存中数据传入 RTL8019AS 双口 RAM 的发送缓冲区,然后设置 TPSR 和 TBCR 启动本地 DMA 将数据发送出去,其流程如图 15.22 所示。

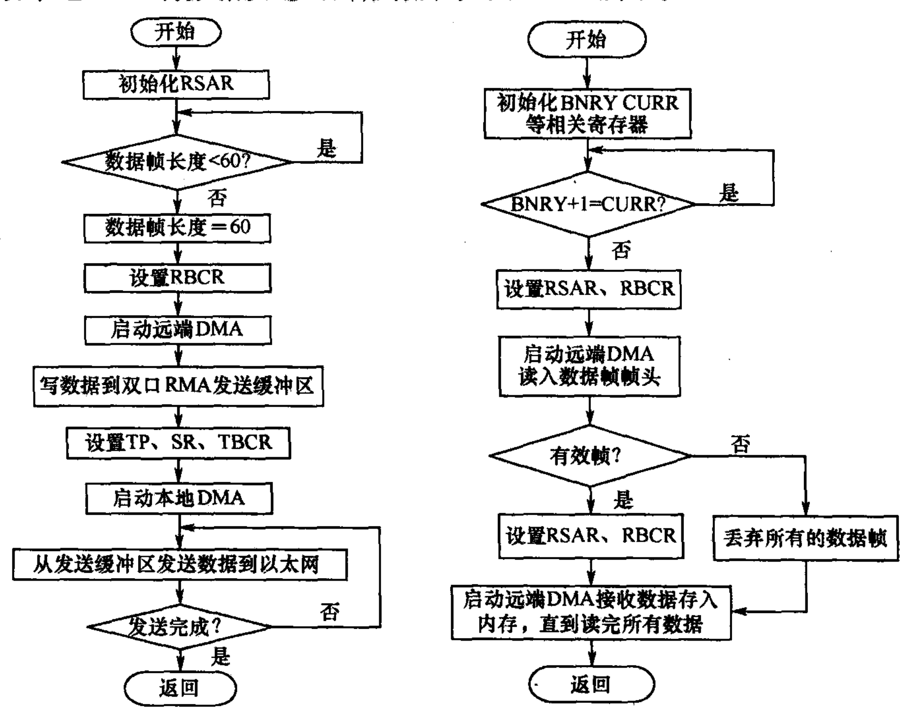


图 15.21　数据帧接收程序流程图　　　图 15.22　数据帧发送程序流程图

15.3.4 电源模块设计

由于 Sink 节点不同于传感节点和簇头节点,它通过网络接口使用 CAT-5 类线与以太网连接,因此基于节点能量供给可持续性和便捷性,Sink 节点的供电模式可以采用以太网供电(Power over Ethernet,PoE)。IEEE 802.3af 标准定义了一种允许通过以太网在传输数据的同时输送 DC 电源的方法。它能安全、可靠地将以太网供电技术引入现有的网络基础设施中,并且和原有的网络设备相兼容,它最大能提供大约 13W 的功率。这样,Sink 节点就可通过以太网连接供电而无需使用电池供电或 AC 电源,从而大大增加了供

电的可持续性并简化了布线,降低了 Sink 节点的构建成本。另外,通过 UPS 备份的局域网供电,还可以使 Sink 节点免受电网掉电的影响,在停电的时候仍然可以运转。以太网供电机理如图 15.23 所示。

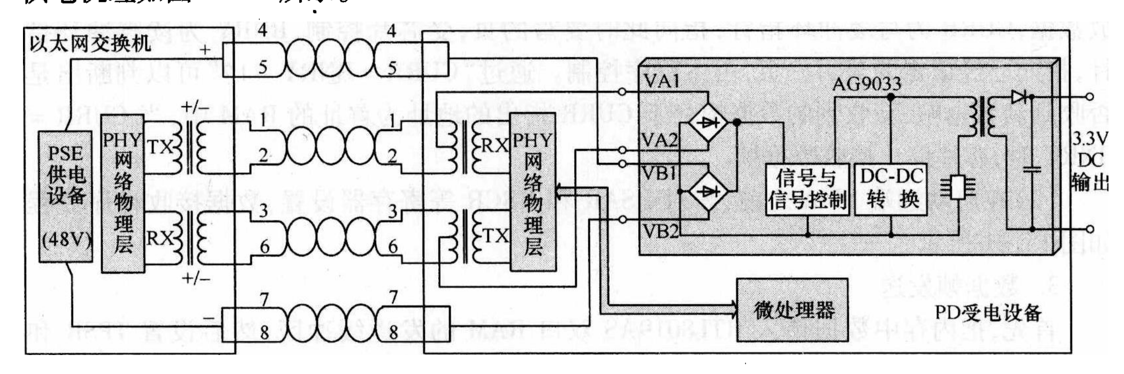


图 15.23　以太网供电机理示意图

图 15.24 为 Sink 节点以太网供电原理电路图,实物图如图 15.25 所示。基本组成为以太网受电转换模块 AG9033、网络隔离变压器 LT01－2006D 和 RJ45 接头,AG9033 的功能是将 48V DC 电压转换为 3.3V DC 电压,并提供 6W 的输出功率。

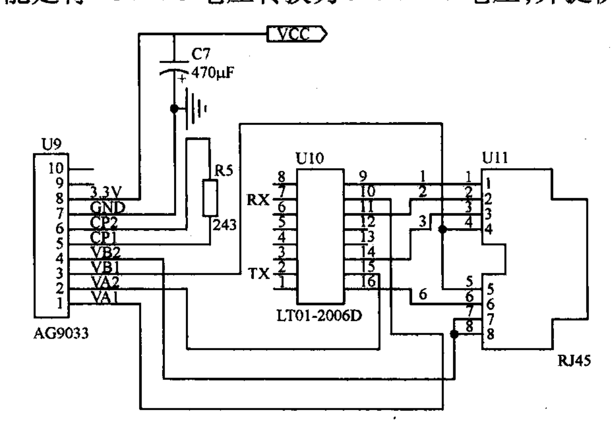


图 15.24　以太网供电原理图

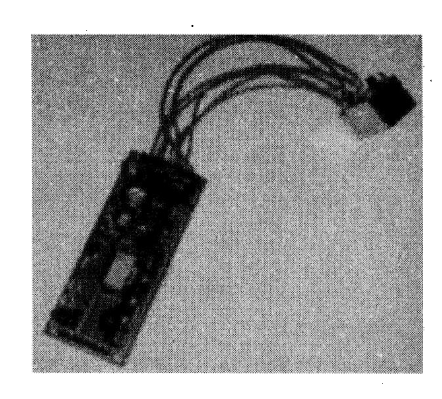


图 15.25　以太网供电模块实物图

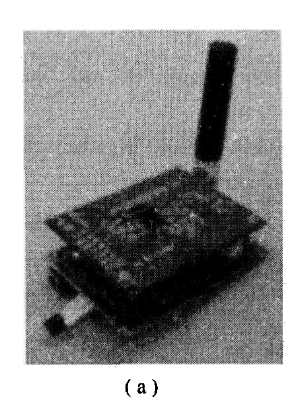
15.4　网络节点系统实现与功耗测试

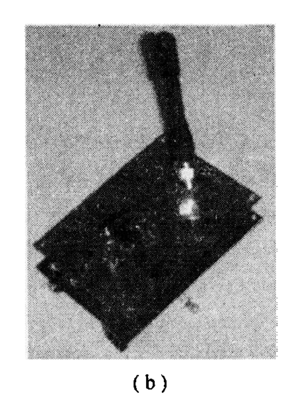
15.4.1　节点系统实现

图 15.26 为传感节点、簇头节点和具有多接口模式 Sink 节点实物图,图 15.27 为无线传感器网络组网实现例图。

15.4.2　传感节点功耗测试

以 3 个传感节点和 1 个 Sink 节点相互收发信息为场景,节点间距为 100m,传感节点采用 3 节 1.5V AA 电池供电,射频频率设定在 915.0MHz,传送功率为 10dBm,试验分别采用如表 15.4 所列的电池容量,系统上电后,以 Sink 节点收到数据为时间起点,以收不


(a)


(b)

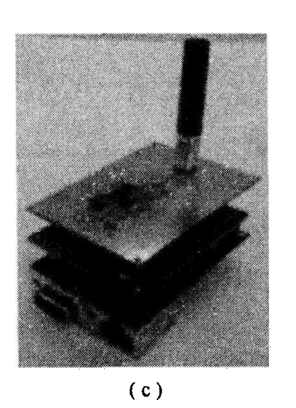
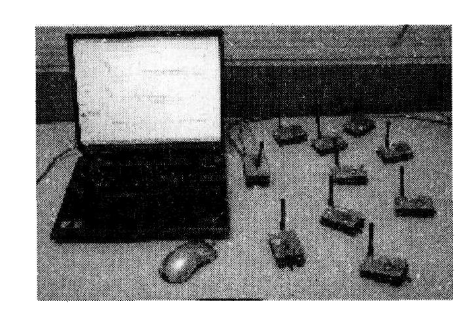

(c)

图 15.26　节点实现图
(a)传感节点;(b)簇头节点;(c)具有多接口模式 Sink 节点。



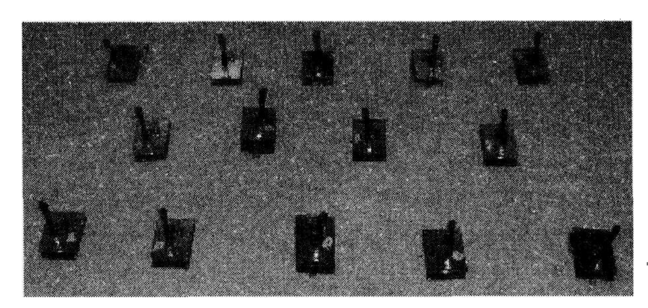


图 15.27　组网实现例图

到数据为时间终点,测试结果如表 15.2 所列,从表中可以看出:

(1)随着电池容量的增大,节点系统的寿命延长。

(2)采用 1% 的占空比使传感节点间歇性工作,由 10h 实测能耗推算出节点的工作寿命大大延长了,采用 3×3000mAh 的 AA 电池供电时,其工作时间将超过一年,可以满足特定应用场合对系统工作寿命的特殊要求。

表 15.2　节点采用不同容量电池供电时系统工作寿命

序号	电池容量 /mAh	工作寿命 /h	连续工作 10 h,占空比为 1% 的节点能耗/mAh	理论推算占空比为 1% 的工作寿命/h	理论推算占空比为 1% 的工作寿命/d
1	3×1000	100	9.16	3275.3	136.5
2	3×1500	150	9.18	5555.6	231.5
3	3×3000	300	9.13	9857.8	410.8

参 考 文 献

[1] 张劼, 景博, 张宗麟,等. 基于嵌入式 Web Server 的无线传感器网络系统设计[J]. 传感技术学报, 2006,19(2): 468-472.

[2] 张劼, 张宗麟. 基于网络的复杂航空系统远程故障自修复自重构信息系统设计[J]. 航空工程与维修, 2007,1:

47 - 50.

[3] Deborah Estrin, Akbar Sayeed, Mani Srivastava. Wireless Sensor Networks[EB/OL]. http://www.cens.ucla.edu/, 2004, 3.

[4] Dimitrios Lymberopoulos, Andreas Savvides. A Wireless Sensor Node Architecture for Exploring Distributed Sensor Network Applications[R]. DRAFT - Work in Progress, 2005.

[5] Heinzelman W, Chandrakasan A, Balakrishnan H. An Application - specific Protocol Architecture for Wireless Micro Sensor Networks[J]. IEEE Trans on Wireless Communications 2002, 4:660 - 670.

[6] Chen Shuai, Zhong Xianxin, Li Xiao yi, etc. Pervasive Reconfigurabl e Sensor Network Instrument[A]. 3rd International Symposium on Instrumentation Science and Technology (ISIST)[C]. 2004,11:1248 - 1252.

[7] Single chip 433/868/915 MHz Transceiver nRF905 [S]. PRODUCT SPECIFICATION, http://www.nvlsi.no, 2002,11.

第 16 章　无线传感器网络原型验证系统

为了实现无线传感器网络工程化应用，构建原型系统十分必要，它有利于验证本书相关理论与技术的实用效果、及时发现实际应用中有关问题、获取相关改进经验，为无线传感器网络进入实用化阶段奠定基础。本章以设计面向智能监测的无线传感器网络原型系统为目标，系统由监测现场、无线传感器网络、因特网和监测中心组成，为给用户提供网络交互接口和多种操作服务支持，需要实现监测系统应用层软件。

完成以上设计后，由航空机载电源实验台提供较为复杂电磁环境和干扰噪声场景，验证原型系统的基本功能，包括原型系统节点硬、软件电磁兼容性与抗干扰能力，系统运行的稳定性和可靠性。最后，通过“可靠性测试设备整体性能监测”工程实用。在原型系统中，簇头为已知，不参与簇头产生的选举算法。当然，这样做的原因是簇头的选举具有独立性，并且不影响原型系统的构建。

16.1　智能监测原型系统体系结构

基于本书提出的两层分簇结构，设计一种如图 16.1 所示的智能监测无线传感器网络原型系统。该系统可实现数据采集、综合状态监测、突发事件处理等应用场景。

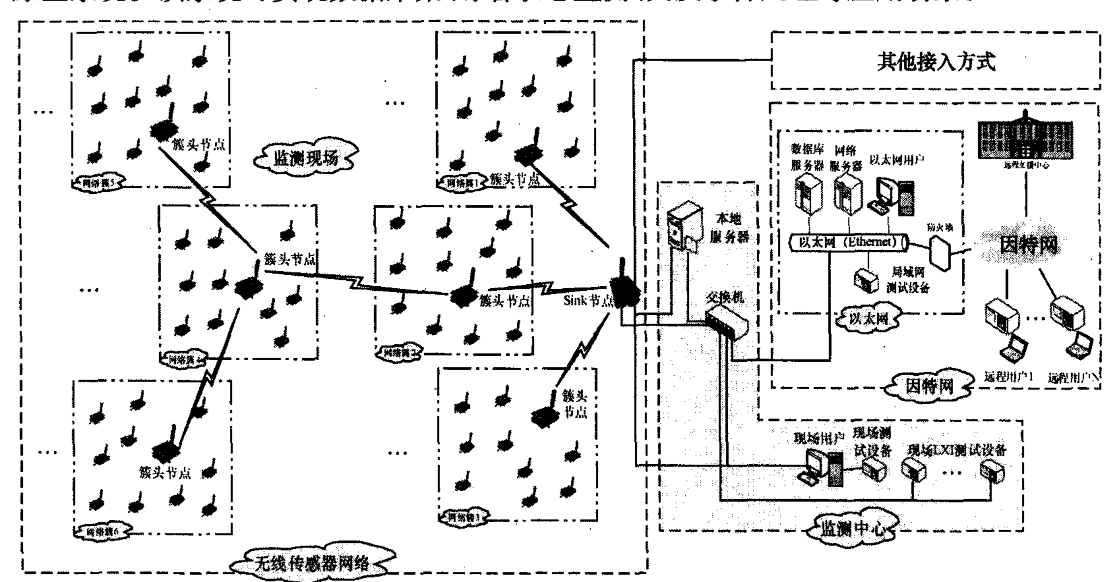


图 16.1　智能监测系统原型

相应的原型系统应用层需处理以下 3 种应用模式：

(1)周期性采样。对于某个需要经常监测的状态或过程，传感器节点每隔一定周期

便进行数据采样,并周期地将采样数据传输到Sink节点,采样周期主要根据状态或过程变化速度以及采集对象自身特点来决定。由于传感器节点的占空比变化与采样速率成正比,协议堆栈的应用层应该在满足测量条件的情况下尽量采用最小采样率。

(2)事件驱动。许多情况下要求监测一个或多个变量,并在接近阈值时才进行传输。为了使事件驱动达到一定的功效和响应速度,必须使没有触发事件的传感器节点进入低功耗模式,并在到达阈值时快速恢复工作。

(3)存储和转发。簇头节点是重要的数据存储和处理节点,通过数据融合降低出口流量,有助于提高整个网络的性能、功耗和带宽效率。应用层协议提供恰当的编程接口,以便有效地集成数据聚集和数据处理方法。

原型系统以"单晶"结构成簇的方式[1]构成无尺度传感器网络系统,其中,簇是网络拓扑结构的基本单元。它具有更好的可控性和安全性,在原型系统中,由于簇头预先可知,因此降低了网络拓扑结构创建和相关网络协议设计的复杂性,有利于网络的维护和长期使用。

本地监测系统通过Sink节点的RS-232C串行接口和RJ45以太网接口接入无线传感器网络。本地服务器实时接收采集数据,并通过多功能监测软件进行数据保存、数据分析和性能监测。此外,还可接入LXI总线测试仪器和设备。

由于需要通过因特网来访问系统采集的各种数据,因此,网络远程交互能力是原型系统提供的一个重要功能。传感器节点采集的原始数据经簇头节点处理后通过Sink节点的RJ45接口接入因特网,从而使网络获取的数据到达远程用户。

16.2　原型系统模块构成与功能描述

图16.1所示原型系统的功能模块有传感器节点、簇头节点、Sink节点、本地/远程监测与分析测试系统、因特网的数据传输系统和用户端(本地与远程用户)。传感器节点、簇头节点、Sink节点采用本书第5章中的节点模型。

该系统具有如下的功能:

(1)感知、采集和存储数据。传感器节点具有感知和采集多种信息类型的能力,采集到的数据可以存储并有效管理,以便及时传送给用户进行数据挖掘和分析。

(2)数据访问与控制。系统运行期间,本地(现场)或远程服务器通过Sink节点对传感器节点进行数据访问和控制,监测系统体现一定的网络交互能力。

(3)节能操作。基于本文设计的节点系统硬、软件,可有效降低系统能耗,延长节点与整个网络系统的生存时间。

传感器节点和簇头节点由电池供电,Sink节点由以太网供电,各节点均参与组网、数据传送和相互通信。传感器节点执行目标感知和数据采样,通过转发其他节点的信息,构成单跳-多跳通信网络。簇头节点和簇内传感器节点通信,负责协调和收集簇内节点的监测数据,并进行初步数据融合,它也可同邻居簇头节点及Sink节点通信,负责将簇内的数据传送给Sink节点,簇头节点与Sink节点之间通过单跳或多跳进行通信连接。

为了实现长期有效的监测,传感器节点、簇头节点、Sink节点、本地服务器和远程服务器等均需要对数据进行存储:传感器节点只是临时存储数据,周期性发给簇头节点后就

不需要了,簇头节点将接收的数据进行存储、融合发给 Sink 节点后也不再需要,而 Sink 节点是监测系统和外界联系的桥梁,需要暂存一定的数据,向本地服务器和远程服务器提供一个比较完善的数据服务。

(1)远程用户可以对本地数据库进行复制和操作。

(2)本地用户直接对网络进行操作,访问每个节点簇,得到传感器网络最新的监测数据。

(3)用户可通过用户界面输入指令调整采样频率、电源管理参数和某些传感器节点执行机构的动作参数来控制传感器网络。

在原型系统中,传感器节点随机均匀部署在监测区域内,簇头节点按照第 8 章中的放置原则放置于监测区域内,Sink 节点根据具体应用环境放置。当没有突发事件出现时,传感器节点对相关信息进行周期性的采集,这时无线传感器网络用于状态监测,采集的信息通过本文设计的通信和路由方式传送到簇头节点和 Sink 节点。当突发事件出现时,传感器节点执行中断处理程序,将突发事件及时上报给簇头节点,簇头节点在 μC/OS - II 调度下,执行优先级最高的中断处理,将突发事件信息及时发给 Sink 节点。

节点时间同步采用 Jeremy Elson 提出的 RBS(Reference Broadcasts Synchronization)策略[2~4],其主要思想是:节点以自己的本地时钟记录事件,文中参考节点选为 Sink 节点,它以广播方式发送一个参考帧给相邻簇头节点,随后其他簇头和簇内各个传感器节点彼此交换收到的参考帧到达时间来计算彼此之间的时间偏移,以此来实现节点之间的同步。它消除了除各个传感器节点自身处理延时以外的各种源错误。

16.3　组网算法设计

16.3.1　网络协议低功耗设计策略

无线传感器网络协议栈的核心部分是数据链路层、网络层和数据融合层协议。数据链路层的关键是 MAC 协议,它控制相邻节点间无线信道的使用方式,决定无线收发模块的工作模式(发送、接收、休眠)。网络层主要是路由协议,负责选择采集信息和控制信息传输路径,MAC 协议和路由协议是影响无线传感器网络能量消耗的重要因素。融合层主要是降低冗余和精确监测数据的融合算法。

1. MAC 层

MAC 协议设计主要考虑以下几方面:

(1)节省能量。由于网络节点数量以及放置环境等因素影响,越来越趋向使用一次性电池,因此要高效地使用电池能量。

(2)可扩展性。节点数目、节点分布的密集程度和网络拓扑结构要具有可扩展性,以适应网络节点个数增加、减少(电池能量耗尽)和位置变化。

(3)网络的公平性、实时性及网络吞吐量、带宽利用率。

网络节点无效功耗主要有 4 个来源:空闲侦听、冲突、串听和控制开销[5]。MAC 协议采用基于预先规划的机制(如 TDMA)来保护节点的能量。其中,射频通信模块是节点中最大的耗能模块,是 MAC 协议优化的主要目标,采用的主要方法是减少数据流量、增加射

频通信模块休眠时间和冲突避免等，其中，减少数据流量是最根本的解决方案。

（1）直接控制射频模块，对节点功耗有重要影响。节点在没有数据接发时，关闭射频模块，转入休眠状态，这种方法可以降低工作占空比，减少串扰和空闲侦听带来的能量浪费，代价是增加了延迟和降低了系统吞吐率。

（2）减少数据流量主要靠在网络层上增加一个数据融合层来实现。

（3）协议越简单越好。

2. 网络层

网络层路由协议以数据为中心，设计目标是能量有效性路径建立和可靠数据转发机制形成。采用基于能耗的路由（节点当前的剩余能量、目标节点与本节点之间的距离等）可以提高能量效率，加快网络冗余数据的收敛。无线传感器网络没有一个全局的标识，一般是基于属性的寻址方式，因此，可采用被动式路由方式。

路由协议要遵循的设计原则如下：

（1）必须将有效利用能源放在第一位，将服务质量放在第二位。

（2）不能执行太复杂的计算，要求协议的帧和算法简单有效，实现的程序代码短小精悍，路由表项尽可能少。

（3）不能在节点保存太多的状态信息，且节点间不能交换太多的路由信息。

（4）以单跳—多跳方式路由，转发数据帧。

（5）尽量避免发送冗余信息，减少能量的浪费。

（6）为了避免单个节点的失效影响整个网络的效率，要求每个节点尽可能维护多条路由，只有当所有路由都失效时，才按需发起路由请求过程，从而降低了路由请求频率、分组等待延时和协议开销。

3. 数据融合层

尽管网络中传感器节点的冗余性是防止在个别节点或链路失效的情况下，引起网络分立或监测数据的不完整，但如果直接把这些原始数据传输给用户集中计算，会造成网络通信量巨大。因此，需要同时考虑传感器节点多源信息的时间性和空间性，将时空域信息进行融合，以剔除冗余数据，提高数据收集效率，降低网络拓扑结构中第2层的数据传输量，并获取更准确的信息。

16.3.2　物理层数据传输协议设计

通信协议是无线网络节点为实现信息交换而制定的通信规则。为了避免同频干扰问题，本节采用TDMA技术将点对多点的通信方式转化为点对点的通信，因此必然涉及信源与信宿建立通信的地址匹配问题。而且由于无线收发模块的特性，通信可能在发射端与接收端之间受到外界的干扰而使数据发生错误，也需要通信协议来保证接收端能正确接收数据，并确定所接收数据是否为实际数据。本通信系统前端的数据采集及处理器为微处理器，在实际智能监测应用中数据的通信量不大，所以通信协议应该以简单和可靠为主，本节主要设计物理层通信协议，物理层通信协议主要完成信号的编码和译码、比特到字节的转换、比特的传输和接收的功能。物理层数据帧与MAC层数据帧的关系如图16.2所示。

物理层主要利用nRF905芯片的串行外围接口SPI高速同步传递数据。SPI耗费很

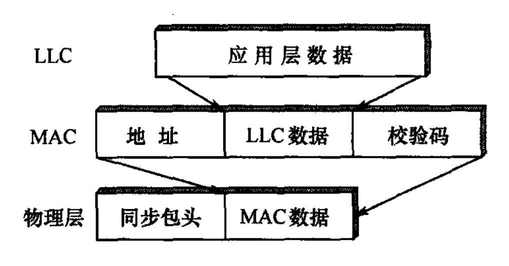


图 16.2　物理层数据帧与 MAC 层数据帧的关系

少的 CPU 时间，CPU 的时钟速度决定数据处理速度，因此这里使用 SPI 传递数据。设计的协议数据包格式如表 16.1 所列。

表 16.1　数据包格式

引导字头	发送字节ID	本节点ID	数据长度	数据块	……	校验码

引导字头是一个同步序列，它确保在地址位和数据位被解调以前接收到正确的直流调制信号，具有稳定接收和同步接收 SPI 的作用。nRF905 采用 5 个字节，引导字头定义为 CCCCCCCCF0h（即 0XCC，0XCC，0XCC，0XCC，0XF0），用于接收数据时同步数据帧。簇头节点接收到传感器节点 ID 后，与本身的 ID 号进行比较，“是”则继续接收数据，“否”则可丢掉后续的数据。本节点 ID 是用来标志发送信息节点的编号。校验位是将除引导字头以外的数据采用校验和方式或更好的 CRC 校验方式，确保节点接收的数据不会由于外界干扰而出错。

编码方式本文采用一种新的动态交错编码（Dynamic Scrambling Coding，DSC），DSC 是简单的对数据字节和代码字节进行逻辑异或的编码方法。

（1）选择 10101010 作为代码字节，11110000 作为数据字节，将它们进行交错编码后就得到 01011010，这就使得通信过程中电平的转换由 1 次变为 6 次，大大增加了通信的可靠性。在接收方，将得到的数据 01011010 与代码 10101010 进行异或就得到初始数据字节 11110000。

（2）当字节 10101010 与代码字节 10101010 进行交错编码后就得到 00000000。显然在这种情况下将使得数据包中原有的电平变化消失，因此不应该使用 DSC。

通信协议应该兼顾各种字节的情况，力求得到任何情况下最多次数的电平转换，本文采用对数据包中的每一个字节开启或关闭的 DSC。按照 DSC 的要求，需要额外的一个标志位，以此来说明是否进行了交错操作，这样 1 个字节的传输需要 9 位，同时为了得到可以变化的传输波特率。在接收方，当接收到 1 个字节时，先要判断第 9 位是否为 1，如果为 1，则需要进行反交错操作才能得到原码。

16.3.3　数据融合算法设计[6,7]

为了获取更精确的感知信息和节约有限的节点能源，在网络路由中应用数据融合是必不可少的，数据融合解决的主要问题是去除冗余网络数据，尽可能减少冗余信息的发送。对于多个同构传感器节点测量任何先验知识未知的同一对象（目标）的情形，将有大量的冗余数据产生。Govindan 的研究表明[6]：在分布密度为 $\rho(x,y)$ 的随机区域 S′内，传感器节点间冗余数据为 $\eta = \xi S' e^{\rho}$，ξ 为冗余系数。如果直接将这些未经处理、存在冗余的

数据进行传输，将会造成网络带宽、节点能源的巨大浪费，导致节点迅速死亡，缩短整个网路的生命周期。

16.3.3.1　簇头节点数据融合算法概述

目前成熟的数据融合算法，如果各个传感器节点测量噪声的方差或先验概率分布已知，可通过基于统计理论的 Bayes 方法[7]，或基于规划的权值最优分配方法[8]融合多个传感器节点的测量值；如果被测对象可以用状态方程和测量方程来描述，可利用 Kalman 滤波及其扩展型[9]融合测量值。尽管这些方法的融合效果都很好，但它们共同的缺点是必须知道测量信息的先验知识，如噪声强度、先验概率分布、关联概率分布等。而智能监测的无线传感器网络特性，决定了测量信息先验知识是未知的[10,11]。因此，必须研究不依赖任何先验知识的融合算法。

【定义 16.1】节点支持度（Node Support Degree）：多个节点测量同一个参量，测量值一般满足正态分布[12,13]，节点之间测量偏差的大小表示节点间的相互支持程度，即置信距离测度，亦称支持度。节点支持度是来表示传感器节点间测量信息一致性的特征量。设置信距离测度为 a_{ij}，a_{ij} 表示第 j 个节点对第 i 个节点的支持程度。

本节基于能量有效性需求，在数据融合层，研究了基于传感器节点支持度的簇头节点一致可靠性融合算法（CRFSD）。该算法模型描述如下：

基于支持度矩阵，运用指数衰减函数度量各传感器节点测量值的支持度，在时间域，根据不同时刻的一致性序列，判断各传感器节点在整个测量时间上的测量可靠性；在空间域，根据某个时刻测量值，判断各传感器节点的测量一致性，并综合利用传感器节点的空间域和时间域信息，对测量值加权，从而实现基于支持度的时空域一致可靠性融合。融合算法在各个簇内分别进行，传感器节点负责将感知数据传送到簇头节点，簇头节点完成融合算法，并将融合结果发送给 Sink 节点。该算法有利于网络用户获取目标状态或过程真实的信息，并做出准确的决策与估计。

16.3.3.2　CRFSD 融合算法设计

由 n 个传感器节点组成的传感器节点阵列，采用直接测量的方法，对静止或渐变参数 X 监测，即

$$z_i(k') = X + v_i(k') \qquad (i = 1, 2, \cdots, n)$$

式中：$z_i(k')$ 为第 i 个传感器节点在 k' 时刻的测量值；X 为目标；$v_i(k')$ 为 k' 时刻的测量噪声，且 $E[v_i]$ 和 $D[v_i]$ 均未知。

如果 $z_i(k')$ 和 $z_j(k')$ 相差较大，表明两个传感器节点的测量值相互支持度低，甚至相互背离，如果 $z_i(k')$ 和 $z_j(k')$ 很接近，表明这两个传感器节点的测量值相互支持度高。为了量化各传感器节点在同一时刻测量值的支持程度，引入指数衰减函数，并构造支持度矩阵。

在 k' 时刻，传感器节点 i 和传感器节点 j 测量值支持度为

$$a_{ij}(k') = \exp(-\chi(z_i(k') - z_j(k'))^2) \tag{16.1}$$

运用指数衰减函数量化传感器节点测量值的支持程度，避免了传统方法中支持度非 0 即 1 的绝对性。另外，χ 为可调参数，调节 χ 的大小，可以方便地调整度量尺度，在程序上易于实现。据此，可得 k' 时刻传感器节点间的支持度矩阵为

$$SD(k') = \begin{bmatrix} 1 & a_{12}(k') & \cdots & a_{1n}(k') \\ a_{21}(k') & 1 & \cdots & a_{2n}(k') \\ \vdots & \vdots & & \vdots \\ a_{n1}(k') & a_{n2}(k') & \cdots & 1 \end{bmatrix} \tag{16.2}$$

对于支持度矩阵 $SD(k')$ 中某行元素来说，若 $\sum_{j=1}^{n} a_{ij}(k')$ 大，则表明 k' 时刻第 i 个传感器节点的测量值与多数传感器节点保持一致；反之，第 i 个传感器节点的测量值偏离多数传感器节点的测量值。

在 k' 时刻，第 i 个传感器节点测量值与其他传感器节点测量值一致性度量为

$$r_i(k') = \frac{\sum_{j=1}^{n} a_{ij}(k')}{n} \tag{16.3}$$

显然，$0 < r_i(k') \leqslant 1$。式(16.1)反映了在某个测量时刻，两个传感器节点测量值的接近程度。式(16.3)反映了在某个测量时刻，第 i 个传感器节点的测量值与所有传感器节点(包括第 i 个传感器节点)测量值的接近程度。

基于式(16.3)测量值的一致性度量，分别从空间域和时空域对传感器节点的测量值进行融合。

1. 空间域数据融合

只考虑某个测量时刻传感器节点测量值一致性度量 $r_i(k')$，不考虑测量值在整个测量区间的可靠性。

若用 $\hat{X}_z(k')$ 表示 k' 时刻簇 z 中 n 个传感器节点测量值融合后对目标的估计，则 $\hat{X}_z(k')$ 可用一致性度量来计算，即

$$\hat{X}_z(k') = \frac{\sum_{i=1}^{n} r_i(k') z_i(k')}{\sum_{i=1}^{n} r_i(k')} \tag{16.4}$$

基于一致性度量对目标融合估计的算法复杂度低，但并未挖掘和利用不同时刻的一致性度量所蕴涵的传感器节点可靠性信息。

2. 时空域数据融合

考虑不同时刻的一致性度量所蕴涵的传感器节点可靠性信息，在空间域的数据融合基础上，引入时间域的节点信息。

在某个测量时刻，传感器节点测量值一致性度量 $r_i(k')$ 很大，但并不能说明在整个测量区间上传感器节点的可靠性高，传感器节点的可靠性是通过所有测量时刻的一致性度量表现出来的。例如，$r_i(k')$ 在某个时刻很大，但某个时刻又变得很小，这说明传感器节点的测量一致性不稳定，即传感器节点在整个测量时间内可靠性差。在对测量值进行融合的过程中，测量一致性大，且测量一致性变化稳定的传感器节点的测量值应赋予大的权值。

不同时刻一致性度量蕴涵的可靠性信息用统计理论中样本均值和方差来研究：

(1)在 k'时刻,第 i 个传感器节点测量一致性均值表示为 $\overline{r_i(k')} = \frac{1}{k'}\sum_{t=1}^{k'} r_i(t)$,为了缩短簇头节点计算时间,节约节点存储空间,可用其递推形式,即

$$\overline{r_i(k')} = \frac{k'-1}{k'}\overline{r_i(k'-1)} + \frac{1}{k'}r_i(k'),\ \overline{r_i(1)} = r_i(1) \tag{16.5a}$$

测量一致性方差表示为 $\sigma_i^2(k') = \frac{1}{k'}\sum_{t=1}^{k'}[\overline{r_i(k')} - r_i(t)]^2$,其递推形式为

$$\sigma_i^2(k') = \frac{k'-1}{k'}\sigma_i^2(k'-1) + \frac{1}{k'-1}[\overline{r_i(k')} - r_i(k')]^2, \sigma_i^2(1) = 0 \tag{16.5b}$$

实际融合过程中,应当充分利用一致性均值大,且一致性方差小的传感器节点的测量信息,即充分利用一致性和可靠性都很高的传感器节点的测量信息。

(2)在 k'时刻,第 i 个传感器节点测量值的加权系数为 $q_i(k')$。

融合过程中,一致性和可靠性都很高的传感器节点的测量信息应充分被利用。因此,第 i 个传感器节点测量值的加权系数 $q_i(k')$ 与$\overline{r_i(k')}$正相关,而与 $\sigma_i^2(k')$负相关。为使 $q_i(k')$非负,选用线性函数度量最终的加权系数 $q_i(k') = [1 - \varphi\sigma_i^2(k')]\overline{r_i(k')}$,$\varphi$ 为可调参数,调节该值可以改变 $\sigma_i^2(k')$对权系数影响的程度。

由此,对于一时间序列 $k'(1), k'(2), k'(3), \cdots, k'(t)$,节点簇 z 中第 i 个传感器的时空融合估计为

$$\hat{X}_z(k') = \frac{\sum_{i=1}^{n} q_i(k')z_i(k')}{\sum_{i=1}^{n} q_i(k')} \tag{16.6}$$

至此,时空域的融合算法建立完毕。式(16.1)~式(16.4)是空间域的融合算法;式(16.1)~式(16.6)是时空域的全套融合算法。

16.3.3.3　CRFSD 融合算法仿真试验与性能评价

以一个簇头节点和 3 个传感器节点为研究对象,3 个传感器节点的 ID 号分别为 ID1、ID2 和 ID3,3 个传感器节点均采集目标温度,真值为 90℃,但节点上传感器的噪声分布未知。簇头节点接收到的温度测量值各为 7 组,如表 16.2 所列。对表 16.2 所列的测量值,分别用空间域融合、时空域融合及时间域平均算法进行仿真,对于空间域融合和时空域融合,指数衰减系数 χ 选取为 0.8;对于时空域融合,φ 取值为 0.01。图 16.3 为 3 种方法的融合结果。

表 16.2　传感器节点测量值(℃)

传感器节点	测量次数												
	1	2	3	4	5	6	7	8	9	10	11	12	13
ID1	89.5	90.3	90.9	90.6	88.9	89.4	90.0	90.2	89.8	89.3	89.7	90.4	90.2
ID2	89.3	87.9	88.1	88.2	90.5	90.4	88.5	89.4	89.9	89.7	90.2	90.6	90.8
ID3	89.7	90.8	89.2	90.0	89.4	89.6	90.1	90.3	90.3	88.7	89.4	90.2	89.9

由融合效果比较图可以看出：

(1)从绝对误差变化过程来看，基于时空域的融合，其绝对误差总体上低于平均法和空间域融合，且绝对误差变化平缓，呈收敛趋势；从空间域的融合结果看，虽然在第 4 个测量时刻，其绝对误差最小，但总体上的绝对误差变化剧烈。这主要是在融合过程中只考虑了测量数据的一致性，而未考虑测量值在整个时间轴上的可靠性的缘故。

(2)传感器节点间测量值的支持程度反映了不同传感器节点对目标测量一致性程度，而不同时刻的一致性度量反映了传感器节点测量值在整个测量区间内的可靠性。时空域的融合综合利用一致性度量序列的均值和方差，构造加权系数，对各时刻测量值融合。由于充分利用了传感器节点在整个测量区间内一致性序列所蕴涵的传感器节点一致性和可靠性信息，因而有较好的融合效果，且算法有效。

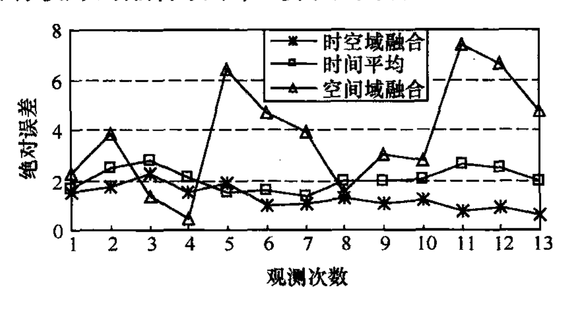


图 16.3　融合效果比较

16.4　监测系统应用软件设计

为了给用户提供一个与无线传感器网络交互的接口，同时也提供对多种操作服务的图形化支持，系统应用层软件必不可少。

1. 软件功能

无线传感器网络智能监测软件采用 C + + Builder 编制，主要完成以下几个功能：

(1)因特网连接。

(2)Sink 节点数据获取。

(3)传感器节点数据实时分类查询。

(4)数据实时动态显示与曲线绘制。

(5)故障报告与定位。

(6)数据保存。

(7)历史数据查询。

(8)网络节点分簇显示。

(9)网络节点信息传递路径查询与显示。

(10)用户信息管理。

(11)报表生成与打印。

(12)系统帮助。提示用户如何使用和维护软件。

2. 软件菜单及功能分布

无线传感器网络智能监测系统功能分布情况如图 16.4 所示。数据采集菜单包括“采集与设置”和“退出”两个子菜单，进入采集与设置菜单，用户选择“连接”后，上位机可采用 XML、JavaApplet 与 Socket 方式和 Sink 节点开始连接，连接成功后上位机动态显示数据采集结果，绘制数据曲线，并提供节点故障报警信息。数据管理部分主要用来查询历史数据，根据传感器节点 ID 号或 IP 地址查询历史记录对用户信息进行管理并生成每次试验报表，此外，还可查询数据传输路径。

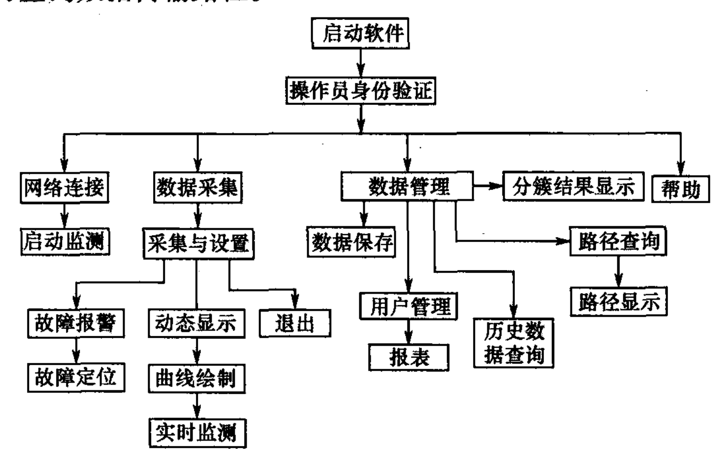


图 16.4　监测系统功能分布

3. 主界面与监测界面

监测软件主界面如图 16.5 所示，数据采集与显示界面如图 16.6 所示，历史数据查询界面如图 16.7 所示。考虑观看舒适性，数据采集与显示界面仅显示 3 个传感器节点数据信息，如若查看其他节点采集情况，可在状态栏输入“节点 ID 号”，数据显示栏则变为所查看传感器节点的相应数据。



图 16.5　无线传感器网络监测系统界面

图 16.6　数据采集与显示界面

4. 分簇查询与路由建立过程查询

由于网络中传递的数据帧和控制帧均包含节点 ID 号信息，因此，监测系统软件提供了网络分簇过程的动态显示和历史回放功能。另外，为了查询某个传感器节点数据路由路径，可通过路径查询界面得到数据传输路径上的节点 ID 及数量。

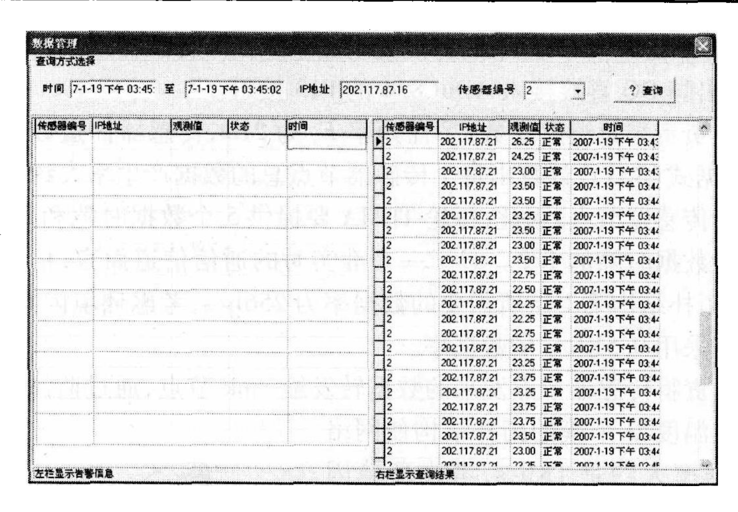


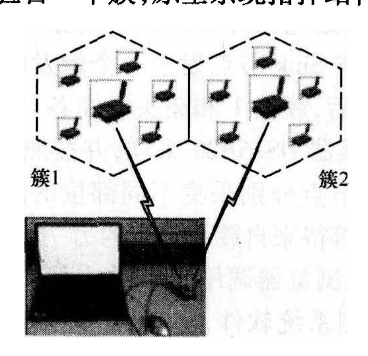
图 16.7　历史数据查询界面

16.5　基于电源实验台的无线传感器网络功能测试床

16.5.1　测试床场景

本节基于航空机载电源实验台的测试床进行温度监测试验，验证原型系统的基本功能。航空机载电源实验台是用于模拟机载发电、供电系统的实验器，由于场景中有大功率的电动机、高转速的航空发电机和多路电磁继电器开关，因此，电源实验台具有较为复杂的电磁环境和干扰噪声，对于无线传感器网络原型系统是一个难得的试验场景。一方面可以验证原型系统中节点硬、软件电磁兼容性与抗干扰能力；另一方面可以检验节点系统的稳定性、协议设计的可靠性和数据传输的准确性。

功能测试床组成包括传感器节点、簇头节点、Sink 节点、电源实验台、监测计算机、集线器和数据采集与分析软件，功能测试床使用两组试验台，无线传感器网络分两个簇，一个试验台一个簇，原型系统拓扑结构及节点放置如图 16.8 所示。



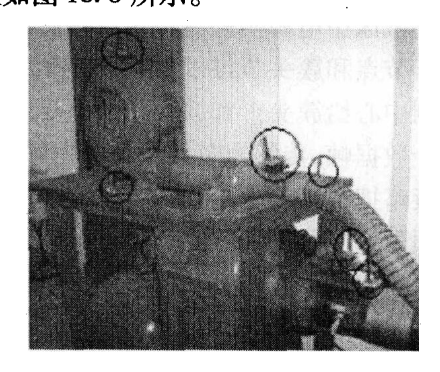


图 16.8　原型系统拓扑结构与节点放置

电源实验台温度监测的验证场景属于小型无线传感器网络的应用，功能测试床中以两个电源试验台为验证对象，监测 5 个部位温度值，温度范围为 -10℃ ~120℃，每个簇内放置 1 个簇头节点和 5 个传感器节点，传感器节点与簇头节点通信半径为 5m，簇头节点

与 Sink 节点通信半径为 12m，且中间有混凝土墙壁遮挡。传感器采用 DS16B20 数字温度传感器，数据输出脚 DQ 直接接入 ADuC834 的 P13 接口。

传感器节点负责采集温度参数，采样频率 F_s 为 2Hz，传感器信道数量 s 为“1”，采样值 t 为 16bit，依据式(8.3)，计算出每个传感器节点总的数据产生率大约是 32b/s，由于每个簇内包含 5 个传感器节点，因此，每轮 TDMA 要提供 5 个数据时隙和 2 个控制时隙，控制时隙的长度为数据时隙的 1/2。对于一个准实时的通信信道而言，信道吞吐量大约是 75%，因此网络拓扑结构第 1 层所需要的数据率为 256b/s，考虑环境因素，原型验证系统第 1 层网络通信采用 0.5Kb/s 的数据率。

簇头节点负责将传感器节点发来的数据转发给 Sink 节点，通过监测计算机实时查看监测部位的工作温度，2 个簇的拓扑结构使网络第 2 层所需数据率大约是 1Kb/s，考虑环境因素，原型验证系统第 2 层网络通信采用 5Kb/s 的数据率，传输速率通过设置 nRF905 来实现。

监测中心由 Sink 节点、集线器和监测计算机组成，Sink 节点和监测计算机通过 5 类信号缆线与集线器连接，连接图如图 16.9 所示。同时将 Sink 节点 RS-232C 串行接口与计算机 RS-232C 串行接口互相连接，通过 2 种连接方式实现数据记录、数据对比和事后数据分析等。

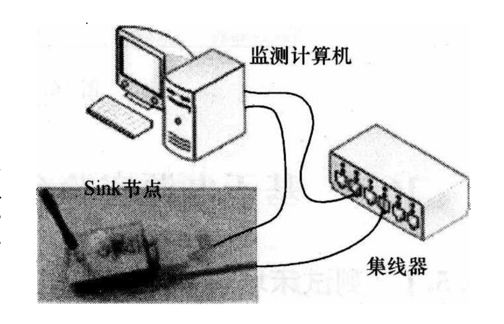


图 16.9　监测中心连接图

通过检测试验现场无线电信号频率，未检测到与 915.0MHz 相近的干扰噪声。

16.5.2　功能性试验与结论

图 16.1 原型验证系统中，簇头 1 内传感器节点 ID 号为 1～5，簇头 2 为 6～10，簇内传感器节点采集的数据分别发给各自的簇头，并由簇头转发给监测机房的 Sink 节点。试验在室温为 13℃的初始温度下开始。

1. 试验一：监测系统周期监测的情形

测试床中电源实验台正常运转后，节点系统上电初始化，时间约为 2s，初始化结束后传感器节点和簇头节点以 RBS 策略时间同步，然后等待 Sink 节点发送一个触发数据帧。在监测中心给簇头 1 和簇头 2 发出要求采样的数据帧后，簇头 1 和簇头 2 在各自簇内广播这个数据帧，传感器节点收到数据帧后利用温度传感器 DS16B20 采样，并按照 FSSMH 路由策略把数据传送给 Sink 节点，簇内的 5 个传感器节点分别采集不同部位的温度，当完成预先定义的采样数之后，传感器节点便停止采样，等待来自簇头节点的另一个采样触发数据帧。显示方式有两种可选：一是通过监测计算机浏览器调用 Sink 节点的测温网页来查看监测结果，如图 16.10 所示。二是通过采集监测系统软件，将 Sink 节点接收到的采集数据图形化显示，监测结果如图 16.11 所示。

功能性试验结论如下：

(1) 监测系统运行后，监测软件界面出现数据图形，IE 浏览器数据窗口显示数据，数据与图形随温度变化而改变，从现场显示来看，两者显示的结果一致，且基本同步。在允许的时延范围内，表明网络监测系统数据采集、传输正常。

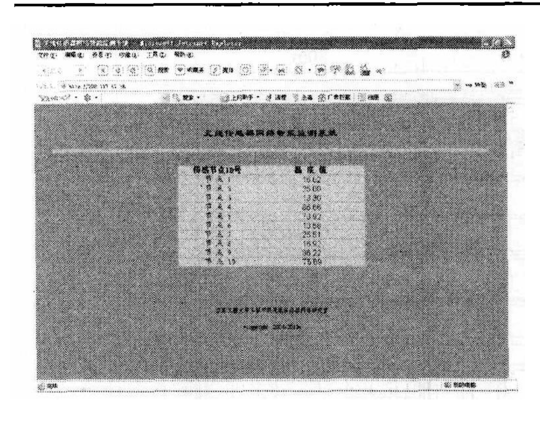


图 16.10　网页显示

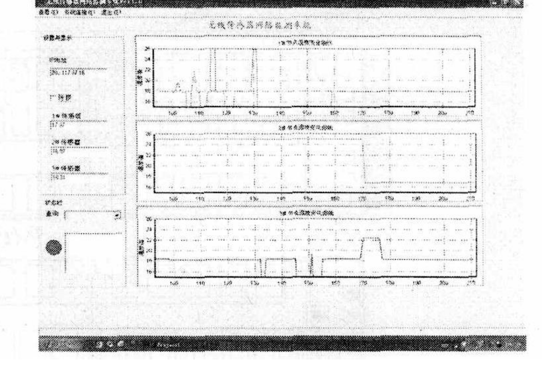


图 16.11　监测结果显示

(2)界面数据显示的变化率体现了一定的实时性。

(3)数据显示未出现乱码,证明节点系统具有较好的硬、软件电磁兼容性。

(4)电源实验台运行 3h 后停机,网络监测系统仍持续工作 72h 后,再次启动电源实验台,5s 后显示界面的数据开始变化,通过长时间工作和负载接入与退出冲击考验,检验了无线传感器网络节点系统的稳定性和可靠性。

2. 试验二:监测系统对突发事件监测的情形

设定 3 号传感器节点报警阈值为 50℃。监测系统启动后,3 号传感器节点最初状态是空闲的,它不监测任何数据。当电源实验台 3 号区域温度达到 50℃ 阈值时,以中断方式触发节点从空闲模式进入工作模式,同时启动无线通信模块的射频装置,向监测中心 Sink 节点发送报警信息和监测数据,收到报警信息状态指示灯闪烁。图 16.12 为 100s 左右时温度超过阈值的示意图。

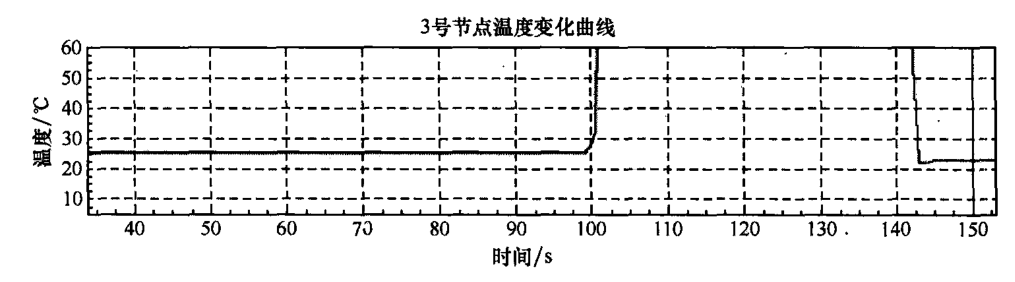


图 16.12　100s 左右超过阈值的温度采集示意图

通过以上两个试验,验证了原型系统的可用性及智能监测应用的可行性。

16.6　可靠性测试设备整体性能监测

16.6.1　监测需求分析

监测中心设备布置场景及设备编号如图 16.13 所示。

监测面积为 98m × 60m,分一个 8m × 28m 监测中心机房和 7 个监测区域(6 个 36m × 28m 大房间,1 个 8m × 28m 小房间),可靠性测试设备尺寸有 8 种,均为规则的长方体,并固定摆放,最大设备尺寸为 5m × 3m × 2.2m,最小设备尺寸为 1.6m × 1.5m × 1.8m。可靠

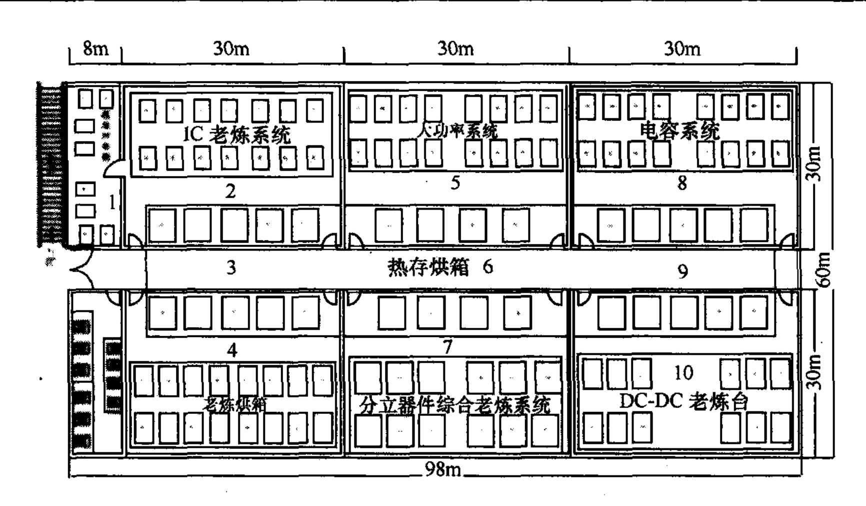


图 16.13　可靠性测试设备分布示意图

性测试设备共有 8 类，共计 122 套，属于中型应用网络，监测状态包括设备性能状态连续集中监测和故障报警，设备种类和具体监测参数指标如表 16.3 所列。

表 16.3　监测参数列表

设备类别	数量	监测参数	参数范围	精度	报警	监测类型
IC 老炼系统	14	温　度/℃	0 ~ 150	3	√	常规测量、突发事件监测、故障报警
		器件老炼电压/ V	-20 ~ 20	0.5	√	
大功率系统	16	器件老炼电压/ V	-40 ~ 40	0.5	√	
		器件老炼电流/ A	0 ~ 10	0.5	√	
电容系统	16	温 度/℃	0 ~ 150	3	√	
		器件老炼电压/V	0 ~ 1200	2	√	
		漏电流/ mA	0 ~ 2	100	√	
分立器件老炼系统	12	器件老炼电压/V	0 ~ 60	0.5	√	
		器件老炼电流/A	0 ~ 3	0.005	√	
DC - DC 老炼台	12	温 度/℃	0 ~ 100	3	√	
热存烘箱	28	温 度/℃	0 ~ 150	3	√	
温度冲击箱	8	温 度/℃	-60 ~ 150	3	√	
		开关量	—	—	—	
老炼烘箱	16	温 度/℃	0 ~ 150	3	√	

8 类测试系统中，IC 老炼系统、大功率系统、电容系统、分立器件老炼系统的工作温度、电压和电流为标准数字信号，可直接接入 ADuC834 的 P1 端口进行测量；热存烘箱、温度冲击箱、老炼烘箱、DC - DC 老炼台的温度信号均为非标准模拟量，信号需要调理到 1V ~ 5V 范围后送入 ADuC834 的 AD 端口进行测量；继电器通断次数是一个开关量，需设计采集调理电路。

16.6.2　传感器节点数据采集硬软件设计

由于表 16.3 中后 4 类设备只能提供模拟信号，因此需要设计调理电路。

1. 温度

温度测量采用 J 型热电偶温度传感器，由于热电偶在 -200℃ ~200℃之间对应的输出电压为 -7.890mV ~10.777mV(中间值参考热电偶分度表)，因此需要采用仪用放大器 AD627 将输出值放大到 1.110 V ~3.077V(参考电压为 2V)，便于传感器节点的 ADuC834 进行采样。此外，由于热电偶测量结果与环境温度有关，因此要对热电偶冷端提供温度补偿，本文采用电流型温度传感器 AD590 测量热电偶冷端温度，并通过软件算法加以补偿，放大调理与温度补偿电路如图 16.14 所示。

传感器节点提供 5 路 AD 输入接口，可同时采集 5 种参数，鉴于 8 类测试系统中最多的需要监测 3 种参数，因此只用 ADuC834 的 3 路 16 位 AD 数据采集接口，16 位采集速率可完全满足应用需要。

2. 开关量

继电器通断次数是开关量，监测方案中采用比较器 LM393 完成测量，继电器接通，Kin 为高电平，反之，Kin 为低电平，传感器节点通过同时采集 P10 和 P11 高、低状态判断继电器的接通与断开，开关量测量电路如图 16.15 所示。

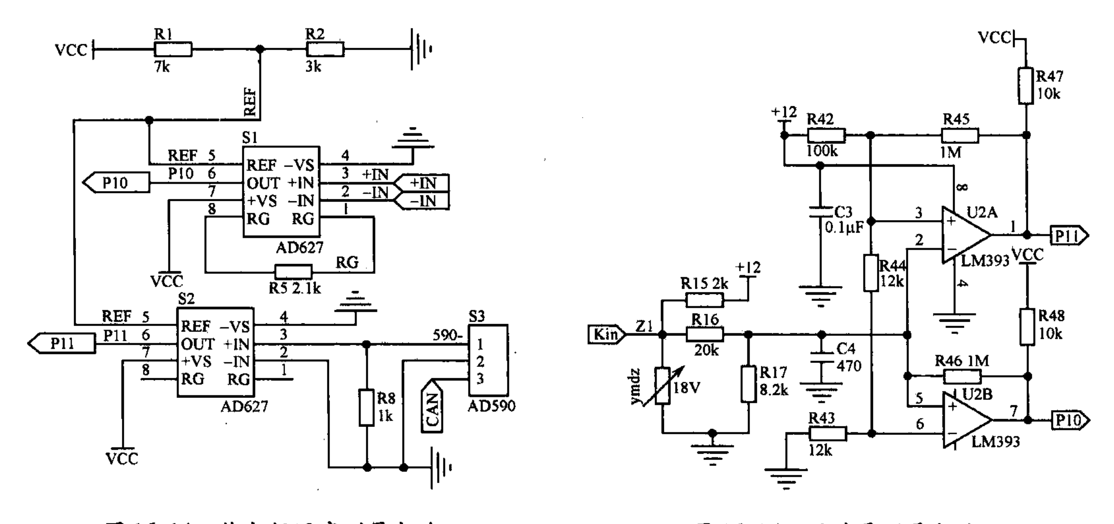


图 16.14　热电偶温度测量电路

图 16.15　开关量测量电路

数据采集与 A/D 通道转换程序流程，如图 16.16 所示。

16.6.3 监测系统体系结构描述

可靠性测试设备整体性能监测按照本章提出的原型组建体系结构，监测系统网络节点放置如图 16.17 所示。

依据原型系统连通与覆盖模型，结合图 16.17 设备布置场景，作如下结构设计：

(1)Sink 节点布置在监测区域中心位置，作为本地控制者没有能量限制，它负责协调和收集簇头节点的数据。

(2)通过参数间的耦合信息，根据监测区域大小、可靠性测试设备分布地理位置、工作区域建筑结构，将热存烘箱划分为 3 个簇，其他每一类检测设备划分为 1 个簇，共计 10 个簇，每个簇放置 1 个簇头，每个可靠性测试设备放置 1 个传感器节点，共 122 个传感器

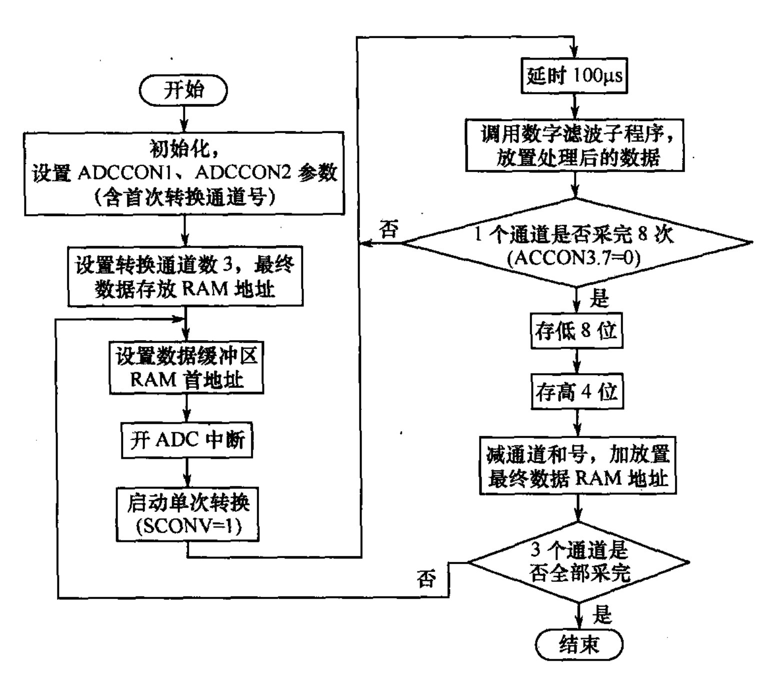


图16.16　数据采集与A/D通道转换程序流程

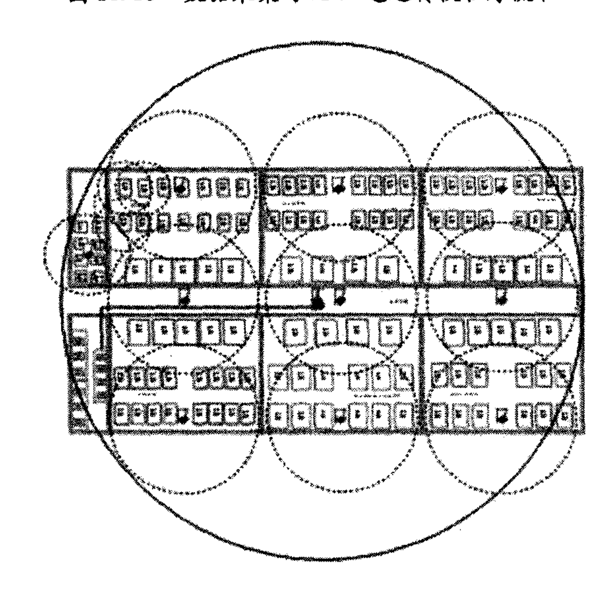


图16.17　监测节点放置场景图

节点，节点编号同设备编号。

(3)考虑每个簇地理区域大小、建筑墙体对射频信号吸附和可靠性测试设备电磁干扰等因素，并考虑能量有效性，设置Sink节点通信半径为50m，簇头节点通信半径为25m，传感器节点通信半径为15m，如此设置可保证簇内覆盖、簇间连通及簇头节点与Sink节点间的通信。传感器节点和簇头节点采用3节1.5V、3000mAh电池供电，Sink节点采用互联网供电。

(4)传感器节点采样周期为300ms，信道数量小于等于3，采样值大小为16bit，簇内传

感器节点数小于等于 16,通过计算可知每个传感器节点总数据产生率(以最大信道值计算)为 0.096Kb/s。每轮 TDMA 通信要提供 16 个数据时隙和 2 个控制时隙(长度为数据时隙的 1/2),对于只有 75% 信道吞吐量的准实时无线通信信道,簇内节点通信所需数据率(以最大传感器节点数计算)为 2.176Kb/s,即网络第 1 层数据率为 2.275Kb/s,则 10 个簇的网络规模使簇头与 Sink 节点之间所需通信数据率大约为 31.8Kb/s,因此监测系统中簇头节点和 Sink 节点通信数据率可采用 100Kb/s,即网络第 2 层数据率达到 100Kb/s,如此设置保证了整个监测系统网络的数据传输。

(5)完成长时间周期性监测和突发事件监测。长时间周期性监测中,传感器节点以低功耗掉电运行模式,通过使能 ADuC834 时间间隔计数器(Time Interval Counter, TIC)中断方式周期唤醒进入工作模式,完成数据采集。当监测设备运行参数超过表 16.3 规定的极限值,传感器节点立即进入中断服务程序,将突发事件数据帧及时路由到 Sink 节点,完成实时故障信息上报。

(6)采用 ASVMAC 信道接入协议、FSSMH 路由协议与算法,考虑监测参数的种类和数量,不使用数据融合算法,以降低系统延迟和计算能量开销。

(7)通过以太网交换机将监测机房内 10 台计算机与 Sink 节点互联,实现 Sink 节点以太网接入,每台计算机安装"无线传感器网络监测系统"用户端软件,便可实时监测可靠性测试设备的运行情况。

16.6.4 监测系统性能测试与运行结果分析

16.6.4.1 系统功能测试与结果分析

设置一个 16B 测试帧由传感器节点以 100ms 周期发送,并由 Packet Sniffer V1.2 软件抓取数据帧加以分析。监测主机配置为 Celeron 2.8GHz CPU。

测试帧格式(hex):|帧头标识|数据长度|节点 ID 号|系统时间|命令标识|数据内容|和校验|帧尾标识|。其中,帧头标识 2B(8D 8D);数据长度 1B,数据帧中除帧头和帧尾标识外所有数据总和;模块 ID 号 4B,传感器节点标识为 ID * *,簇头节点表示为 IDC * *;系统时间 4B,包括日、时(24h 方式)、分和秒;命令标识 1B,为数据帧含义;数据内容 1B(01);校验和 1B,所有数据相加后低字节取补(累加和低字节为 00);帧尾标识 2B(8D 0D)。

监测网络性能测试与评价使用以下 3 个标准。

1. 网络整体能量使用均衡性

从整个网络角度分析节点的能量使用情况,它反映网络算法延缓整个网络寿命的能力,衡量标准为

$$\text{能量使用均衡性} = \sqrt{\sum_{\text{节点数}}\left[\left(\frac{\text{某一时刻所有节点的剩余能量}}{\text{节点总数}}\right)-\text{某一节点的剩余能量}\right]^2} \tag{16.7}$$

表 16.4 为网络节点周期性发送数据帧时,依据式(16.7)计算的节点能量均衡性,并由表 16.4 得到图 16.18,从表和图中可看出,整个网络系统表现出较好的能量使用均衡性,首先,验证了基于 TDMA 通信方式的 ASVMAC 信道接入协议是有效的,由于采用最低能量节点休眠的选举算法,网络能量得到有效均衡;其次,验证了 FSSMH 路由协议设计是有效的,尤其是单跳与多跳算法的实现,均衡了节点能量消耗的速度,使网络生命周期得

到有效延缓。

表 16.4　节点能量均衡性(J)

回合数	10	20	30	40	50	60	70	80	90	100	110	120	130
均衡性	0.25	0.27	0.34	0.23	0.24	0.26	0.30	0.33	0.27	0.25	0.28	0.38	0.36
回合数	140	150	160	170	160	190	200	160	220	230	240	250	260
均衡性	0.29	0.28	0.26	0.29	0.31	0.28	0.27	0.31	0.33	0.31	0.30	0.34	0.29

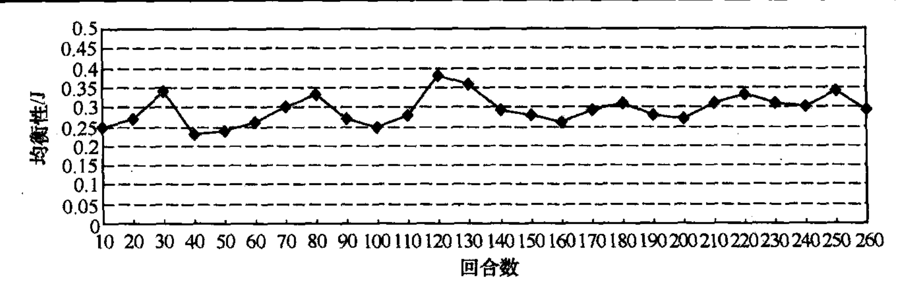


图 16.18　不同回合数网络能量均衡性

2. 数据帧由传感器节点传输到 Sink 节点的成功率

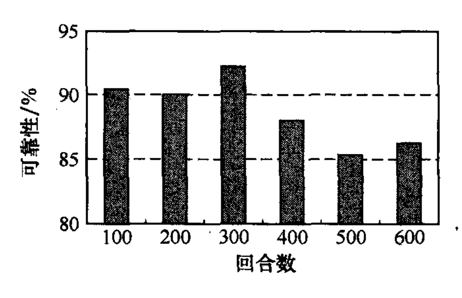
监测中心监测的数据来自 Sink 节点，因此只有传输到 Sink 节点的数据帧对于用户才有实际意义，数据帧由传感器节点传输到 Sink 节点的成功率体现了网络路由算法改善数据传输可靠性的能力，衡量标准为

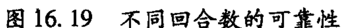
$$\text{数据传输可靠性} = \frac{\text{Sink 节点收到的有效数据帧}}{\text{Sink 节点收到的所有数据帧}} \times 100\% \tag{16.8}$$

通过抓包软件分时计算所抓取的帧总数和有效帧数，并根据每帧时间信息计算出所有节点单位帧平均路由时间，如表 16.5 所列。由表 16.5 得到图 16.19 和图 16.20，从图 16.19 中可以看出，在回合数较少时，数据传输的成功率较为稳定，基本稳定在 90% ~ 95%之间，主要原因是网络运行初期，所有节点的能量都很充足，FSSMH 协议无尺度路由的特点保证了数据传输的成功率；随着回合数的增加，数据传输的成功率下降，主要原因是有些节点能量消耗偏大，基于能量均衡性考虑，按照 ASVMAC 协议休眠能量最低的节点，路由路径不断改变，可靠性略有下降。从图 16.20 中可以看出，完成从传感器节点到 Sink 节点单位帧的平均路由时间小于 300ms，可以满足可靠性测试设备整体性能监测的需求，随着回合数的增加，平均路由时间变化并不剧烈，可见所设计的无线传感器网络是稳定和实用的。

表 16.5　测试帧参数

回合数	收到帧总数	有效帧数	单位帧平均路由时间/ms (包括互联网延迟)	数据传输 平均可靠性
100	1230203	1112612	255.6	90.44
200	2557896	2302753	219.2	90.03
300	3809816	3568173	246.8	93.66
400	4698335	4135661	269.3	88.02
500	5974650	5098634	287.4	85.33
600	7086142	6110826	239.2	86.24




图 16.19 不同回合数的可靠性

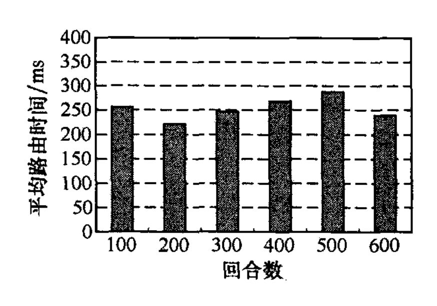


图 16.20 不同回合数的平均路由时间

此外,表 16.5 中有效帧数与总帧数的差距,也反映出节点平台的抗干扰性有待进一步提高,并且路由协议及算法还较为复杂,且忽略了某些客观因素,导致部分数据帧路由出现差错。

3. 每个由传感器节点成功传输到 Sink 节点的数据帧能量代价

这个标准反映出网络使用能量的效率情况,对于硬、软件设计合理的无线传感器网络,只有将主要能量用在传输到 Sink 节点的数据帧上才有效,衡量标准为

$$\text{能量代价} = \frac{\text{所有节点的初始能量} - \text{某一时刻所有节点的剩余能量}}{\text{成功传输到 Sink 节点的有效数据帧}} \tag{16.9}$$

表 16.6 为网络节点周期性发送数据帧时,每一回合随机一个时刻的网络节点剩余能量经式(16.9)计算的能量代价。由表 16.6 得到图 16.21,从图中可以看出,网络表现出较好的能量使用效率,一方面反映了由于 ASVMAC 协议避免了节点数据传输的串扰和冲突重发,有效数据帧数量较高;另一方面,FSSMH 协议无尺度路由和单跳 - 多跳算法的运用,使网络节点剩余能量和成功传输到 Sink 节点的有效数据帧匹配较好,体现了网络运行的可靠有序,能量的有效使用可延长网络生命周期,减少人参与的维护。

表 16.6 节点能量代价(J)

回合数	10	20	30	40	50	60	70	80	90
能量代价	0.046	0.05	0.052	0.048	0.053	0.05	0.047	0.049	0.045
回合数	100	110	120	130	140	150	160	170	160
能量代价	0.049	0.052	0.053	0.051	0.046	0.048	0.047	0.052	0.051
回合数	190	200	160	220	230	240	250	260	
能量代价	0.047	0.049	0.046	0.052	0.05	0.048	0.048	0.052	

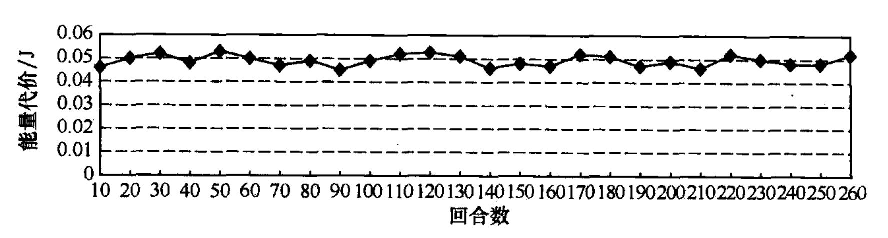


图 16.21 不同回合数的能量代价

16.6.4.2 监测系统运行

图 16.22、图 16.23 是智能监测系统设备监测参数曲线,并有低能量和故障节点报警

提示。

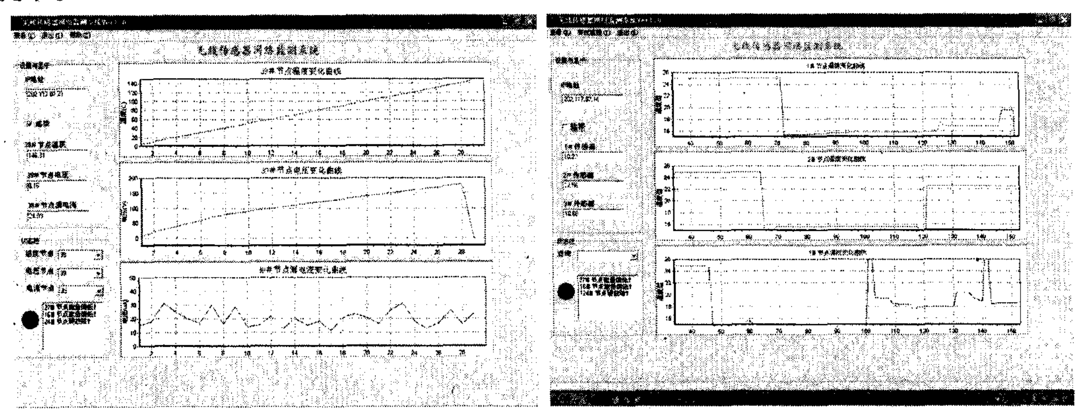


图 16.22　39 号传感器节点 3 种参数监测结果　　图 16.23　不同传感器节点温度冲击监测结果

参考文献

[1] 梁英，于海斌，曾鹏．无线传感器路由协议[J]．信息与控制，2005，34(6)：325－330.

[2] 张劼，孙勇．分布式无线传感器网络及其应用核心技术研究[J]．测试技术学报，2005，2：161－165.

[3] Elson J，Estrin D．Time Synchronization for Wireless Sensor Networks[A]．Proceedings of the 2001 International Parallel and Distributed Processing Symposium (IPDPS)，Workshop on parallel and Distributed Computing Issues in Wireless and Mobile Computing[C]．San Francisco，Califomia，2001，4.

[4] Elson J，Girod L，Estrin D．Fine-grained Network Time Synchronization Using Reference Broadcasts[A]．Proceedings of the Fifth Symposium on Operating systems Design and implementation[C]．Boston. MA，2002.

[5] Arisha K，Youssef M，Younis M．Energy-Aware TDMA Based MAC for Sensor Networks，IEEE Workshop on Integrated Management of Power Aware Communications，Computing and Networking (IMPACCT 2002)，2002，5.

[6] Jie Zhang，Bo Jing，Yong Sun．Calibration Model of the Output Characteristic for Sensor Nodes Based on CMAC Neural Network，Proceedings of the 7th World Congress on Intelligent Control and Automation，June 25－27，2008，Chongqing，China，4995－4998.

[7] 张劼．无线传感器网络体系结构及关键技术研究[D]．西安：空军工程大学，2007，7.

[8] Govindan，Ramesh，Shenker，etc．Highly Resilient，Energy Efficient Multi-path Routing in Wireless Sensor Networks [A]．Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing：MobiHoc [C]．2001，251－254.

[9] 孙勇，张劼，景博．基于支持度的多传感器一致可靠性融合[J]．传感技术学报，2005，16(3)：537－539.

[10] 孙勇，景博，张劼．最优加权与递推最小二乘法相结合的多传感器信息融合[J]．传感技术学报，2004，17.(4)：630－632，654.

[11] Jie Zhang，Bo Jing' Zonglin Zhang. Research on Spatial-Temporal Information Fusion System for sensor networks Node Cluster[A]. the 6th World Congress on Intelligent Control Automation (WCICA06)[C]. IEEE Robotics and Automation Society，2006. 4：3188－3193.

[12] 孙勇，张劼，景博．一种改善分布式参数检测数据性能的新方法[J]．电测与仪表，2004，41(6)：8－10.

[13] Shu-li Sun．Multi-sensor Optimal Information Fusion Kalman Filters with Applications[J]．Aerospace Science and Technology，2004，8：57－62.

第 17 章　无线传感器网络模拟器

在研究无线传感器网络的过程中设计新的协议时，需要对这些协议的性能进行合理评估。目前，常用的协议性能评估方法大致有数学建模分析法（Mathematical Modeling Analysis）、测试床法（Test bed）和模拟器法（Simulator）3 种。

数学建模分析法依赖于数学理论基础和传感器网络的数学模型，可得出相对精确的结果。进行数学分析前，首先需要建立一个合理的数学模型对网络进行描述或抽象。这种模型的建立，大都是无法兼顾各种情况的。因此，采用数学分析法对网络的性能进行评估时，往往还需要具体的实践来证实分析的有效性。

测试床法就是利用物理节点布置实际的网络，在实际网络平台上利用现实的环境，验证网络性能。这种方法对小规模的网络比较适用，但无线传感器网络具有超大规模的特点，难以布置大量的实际节点对网络性能进行测试和评估[1]。

模拟器法是一种将某些网络环境量化后，通过计算机来进行模拟的方法，它可以利用软件模拟硬件环境，有效节省网络协议性能评价的代价。在部署实际的无线传感器网络之前，利用模拟器评估网络性能，对于充分发挥实际网络的效能有重要的现实意义。

17.1　常用模拟器原理及特点

17.1.1　无线网络模拟器

常用的无线网络模拟器有 Ns－2[1]、SensorSim[2]、GloMoSim[3]、OPNET[4]、SENSE[5]、TOSSIM[6]和 Shawn[7]等。

Ns－2 是一个被广泛使用的、离散事件驱动的网络模拟与分析工具，包含一系列协议、流量和 TCP 仿真工具，主要用于 ISO/OSI 模型的仿真。它是位于美国加州的 Lawrence Berkeley 国家实验室于 1789 年开始开发的软件。NS 是一种可扩展、可配置和可编程的事件驱动的仿真工具，它是由 REAL 仿真器发展而来。作为事件驱动的网络仿真软件，NS 可以提供有线网络、无线网络中链路层及其上层，精确到数据包的一系列行为的仿真。

NS 中的许多协议代码都和实际网络中的应用代码十分接近，其真实性和可靠性高居世界仿真软件的前列。NS 底层的仿真引擎主要由 C＋＋编写，同时利用 MIT 面向对象工具命令语言（OTCL）作为仿真命令和配置的接口语言。网络仿真的过程由一段 OTCL 的脚本来描述，这段脚本通过调用引擎中各类属性、方法，定义网络的拓扑，配置源节点、目的节点，建立链接，产生所有事件的时间表，运行并跟踪仿真结果，还可以对结果进行相应的统计处理。

从用户角度看，NS 是一个仿真事件驱动的，具有网络组件对象库和网络配置模块库的 OTCL 脚本解释器。NS 中编译类对象通过 OTCL 连接建立了与之对应的解释类对象，这样，用户在 OTCL 空间能够方便地对 C＋＋对象的函数和变量进行修改与配置。

通常情况下,NS 仿真器的工作从创建仿真类的实例开始。仿真器类可以看成是对整个仿真器的封装,仿真器调用各种方法生成节点,进而构造拓扑图,对仿真的各个对象进行配置,定义事件,然后根据定义的事件,模拟整个网络活动的过程。在创建仿真气对象时,构造函数同时也创建了一个该仿真器的事件调度。

仿真器封装了以下功能模块:

(1)事件调度器。由于 NS 是基于事件驱动的,调度器也成为 NS 的调度中心,可以跟踪仿真时间,调度当前事件链中的仿真事件并交由产生该事件的对象处理。目前,NS 主要提供了 4 种具有不同数据结构的调度器,分别是链表、堆、日历表和实时调度器。

(2)节点。复合组件在 NS 中可以表示端节点和路由器。每个节点具有唯一的地址,节点有单播节点和组播节点两种类型,通过节点内部的节点类型变量来区分。节点为每个连接到它的节点分配不同的端口,用于模拟实际网络中的端口;另外,节点包含路由表以及路由算法,由地址分类器根据目的地址转发数据包。

(3)链路。由多个组件复合而成,用来连接网络节点。所有链路都以队列的形式管理数据包的到达、离开和丢弃,可以跟踪每个数据包到达、进入、离开队列以及被丢弃的时间;还可以用队列监视器监测队列长度和平均队列长度的变化。

(4)代理。负责网络层数据包的产生和接收,也可以用在各个层次的协议实现中。代理类包含源及目的节点地址,数据包类型、大小、优先级等状态变量,并利用这些状态变量来给所产生数据包的各个字段赋值。每个代理链接到一个网络节点上,通常连接到端节点,由该节点给它分配端口号。

(5)包。由头部和数据两部分组成。头部包括 cmn header、ip header、tcp header、rtp header 及 trace header 等,其中最常用的是通用头结构 cmn header,该头结构中包含唯一标志符、包类型、包的大小以及时间戳等。头结构的格式是在仿真器创建时初始化的,各头部的偏移量被记录下来。在代理产生一个包时,所有的头部都被生成,用户能够根据偏移量存取各头部所包含的信息。

基于不同的分工,NS 软件平台主要采用两种开发语言:

(1)具体协议的模拟与实现,需要一种程序设计语言,用于高效率的信息处理和算法执行。为了实现这个任务,程序内部模块的运行速度是非常重要的,而仿真设置时间、寻找和修复程序漏洞的事件及重新编译和运行的时间就显得不是很重要了。

(2)许多网络中的研究工作都围绕着网络组件和环境得具体参数的设置和改变而进行得,需要在短时间内快速开发和模拟网络场景,发现和修复程序中的漏洞,在这种任务中,仿真设置与修改时间就显得非常重要。

因此,为了满足以上两种不同任务的需要,NS 的设计实现使用了两种程序设计语言,C + + 和 OTCL。C + + 语言被用来实现网络协议,OTCL 语言被用来配置仿真中的各种参数,建立仿真的整体结构。

因为 C + + 的特点是具有更快的运行速度,但较为复杂,每次修改代码均需要重新编译,比较适合处理繁琐但比较固定的工作,即上文描述的第一类问题;而 OTCL 虽然在运行速度上无法和 C + + 比拟,但 OTCL 是无强制类型的脚本程序编写语言,容易实现和修改,容易发现和修正程序中的漏洞,相对来说更加灵活,可以很好地解决上述的第二类问题。同时,在 NS 中 C + + 和 OTCL 之间可以通过 TCLCL 工具包自由地实现相

互调用。

NS 总体结构如图 17.1 所示。

Ns－2 源码公开，通过加入感知通道模型、传感器模型、电池模型、轻量级协议、混合仿真支持和场景产生工具等，使其适用于无线传感器网络的仿真。由于源码开放，NS 的使用较为灵活，用户完全可以依据实际需求建立自己的仿真平台。然而，NS 的复杂性一直以来成为它广泛应用的最大障碍。这一仿真软件对用户的编程能力、实际网络协议的理解能力要求较高。而且，NS 的图形化程度较低，使用时往往需要大量修改底层驱动程序，对统计数据的操作也比较困难。

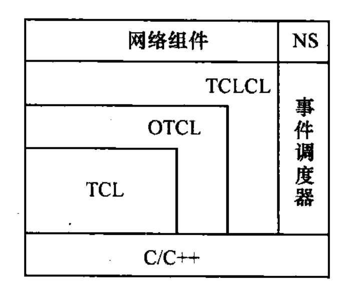


图 17.1 NS 总体结构图

SensorSim 是继承了事件驱动模拟特点的混合式模拟器，一方面通过对运行在实际节点操作系统平台上的应用程序和网络协议混合仿真，利用脚本语言 Tcl 编写中间件 SensorWare 实现两者的协调；另一方面，通过代理和网关机制，对由实际节点和虚拟节点构成的网络进行仿真。

GloMoSim 是一个可扩展的用于有线和无线网络的仿真模拟平台，它采用 Parsec 进行开发，支持并行离散事件的仿真。尽管该平台的理论容量可达到 100000 个节点，但在单一处理器上对 5000 个节点进行模拟，运行时间就长达 1h。

OPNET 是在 MIT 研究成果的基础上由 MIL3 公司开发的网络仿真软件产品。OPNET 网络仿真软件系列需要包括以下 4 个产品：

(1) Planner。也称 IT DecisionGuru，是一个独立的网络规划设计工具，不具有网络节点和协议建模功能，仅限于基于基本模型库的网络建模和模拟。

(2) Modeler。是 MIL3 公司的拳头产品，是一个功能十分强大的网络仿真环境，支持网络中各层设备、链路和协议的精确建模，并提供丰富的外部开发接口，同时还含有 Planner 的全部功能。

(3) Modeler/Radio。在 Modeler 的基础上增加对无线和移动网络仿真的支持，目前可支持移动通信、卫星通信和无线局域网等。

(4) OXD。利用协仿真技术，在网络环境模拟中验证硬件的设计。

OPNET 具有丰富的统计量收集和分析功能。它可以直接收集各个网络层次的常用性能统计参数，并有多种统计参数的采集和处理方法，还可以通过底层网络模型编程，收集特殊的网络参数。OPNET 还有丰富的图表显示和编辑功能、模拟错误提示和告警功能，能够方便地编制和输出仿真报告。

OPNET 采用网络、节点和过程 3 层模型实现对网络行为的仿真，其无线模型采用基于流水线的体系结构来确定节点间的连接与传播。OPNET 提供了多种模型，包括 TCP/IP、802.11、3G 等，但 OPNET 本省更注重对网络 QoS 的评估，要实现对无线传感器网络的仿真，则需要添加能耗模型、MAC 协议等。

SENSE 模拟器提供了众多的电池模型、简易网络模型、应用层模型和 802.11 协议的实现。目前，SENSE 未采用并行仿真引擎，网络规模相对较小。

TOSSIM 在 bit 级对运行 TinyOS 操作系统的 Mote 进行模拟，是一个与硬件平台相关

的模拟器。运用该模拟器可直接将代码在 PC 上编译成可执行文件,无需将代码下载到实际硬件节点上。其缺点是未提供能量模型,无法对能耗有效性进行评价。TOSSIM 的体系结构如图 17.2 所示。

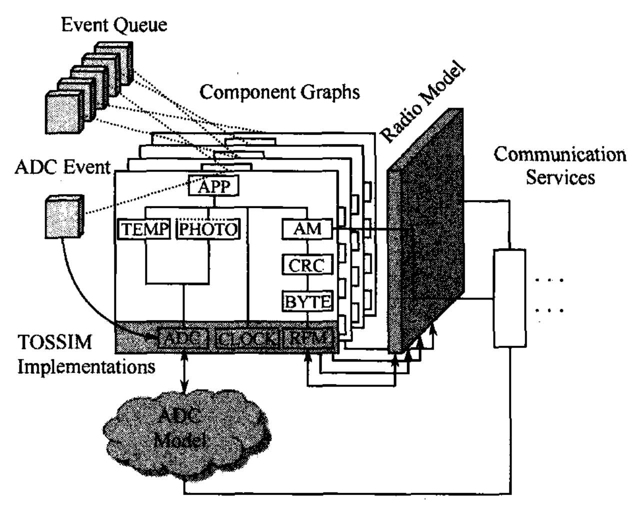


图 17.2　TOSSIM 体系结构:框架、事件、模型、组件及服务

TOSSIM 运用和节点硬件相同的代码,仿真编译器能直接从 TinyOS 应用的组件表编译生成仿真程序。通过替换 TinyOS 下层部分硬件相关的组件,TOSSIM 把硬件中断转换为离散仿真事件。由仿真器事件队列抛出的中断来驱动上层应用,其他的 TinyOS 组件尤其是上层的应用组件都无须更改,因此,用户无需为仿真另外编写代码。TOSSIM 具有以下几个特点:

(1)编译器支持。TOSSIM 改进了 nesC 编译器,通过使用不用的选项,用户可以把在硬件节点上运行的代码编译成仿真程序。编译器支持可同时提供可扩展性和仿真的真实性。

(2)执行模型。TOSSIM 的核心是一个仿真事件队列。与 TinyOS 不同的是,硬件中断被模拟成仿真事件插入队列,仿真事件调用中断处理程序,中断处理程序又可以调用 TinyOS 的命令或出发 TinyOS 的事件。这些 TinyOS 的事件和命令处理程序又可以生成新任务,并将新的仿真事件插入队列,重复此过程直到仿真结束。

(3)硬件模拟。TinyOS 把节点的硬件资源抽象为一个个组件。通过将硬件中断转换为离散仿真事件,替换硬件资源组件,TOSSIM 模仿了硬件资源组件的行为,为上层提供了与硬件相同的标准接口。硬件模拟为仿真物理环境提供了接入点,通过修改硬件模拟组件,可为用户提供各种性能的硬件环境,满足不同用户的需求。

(4)无线模型。TOSSIM 允许开发者选择具有同步精度和复杂度的无线模型,该模型独立于仿真器之外,保证了仿真器的简单和高效。用户可以通过一个有向图指定不同节点对之间通信的误码率,表示在该链路上发送一比特数据时可能出错的概率。对同一个节点来说,双向误码率是独立的,从而使模拟不对称链路成为可能。

(5)仿真监控。用户可以自行开发应用软件来监控 TOSSIM 仿真的执行过程,二者通过 TCP/IP 通信。TOSSIM 为监控软件提供实时仿真数据,包括在 TinyOS 源代码中加入的

DEBUG 信息、各种数据包和传感器的采样值等，监控程序可以根据这些数据显示仿真执行情况。同时允许监控程序以命令调用的方式更改仿真程序的内部状态，达到控制仿真进程的目的。TinyViz(TinyOS Visualizer)就是 TinyOS 提供的一个仿真监控程序。

Shawn 也是一种源码公开的离散事件网络模拟平台，用于大规模无线传感器网络的仿真，既支持高层的算法，也支持分布式协议。在实际仿真过程中，该模拟器配置过程较为复杂，且与操作系统有关。Shawn 核心组件结构如图 17.3 所示。

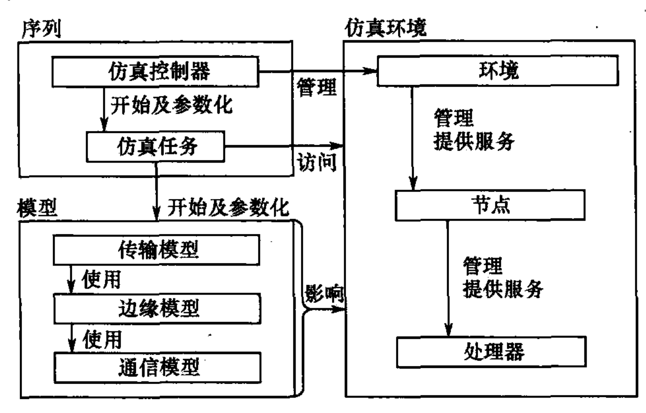


图 17.3　Shawn 核心组件结构

A. Kroller 在文献[7]中对上述几种模拟器性能进行比较，如图 17.4 所示。

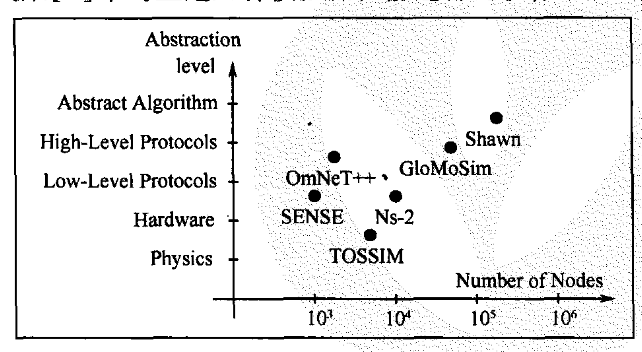


图 17.4　典型无线网络模拟器性能比较

此外，文献[8]给出一种基于 SensorSim 和 ESyPS 两种模拟器的联合模拟框架，其原理是利用 ESyPS 对传感节点的模拟能力，编写两种模拟器通信的 API 函数，连接无线信道和感知信道，并在两者之间进行同步，实现 SensorSim 对无线传感器网络的模拟。

17.1.2　无线传感器网络模拟器

针对无线传感器网络的特点，在现有无线网络模拟器的基础上，研究人员开发了 WINDS[9]、EmStar[10]、SEMU[11]等专门用于无线传感器网络仿真的模拟器。

WINDS 是基于 Linux 操作系统开发的模拟器，支持单一 PC 平台模拟和局域网形式的分布式模拟。通过将模拟任务分配到网络的多个 PC 中，可提高对大规模网络仿真的能力。为了实现各 PC 之间仿真进程的同步，WINDS 利用高速交换机实现 PC 之间的通信。WINDS 体协结构如图 17.5 所示。

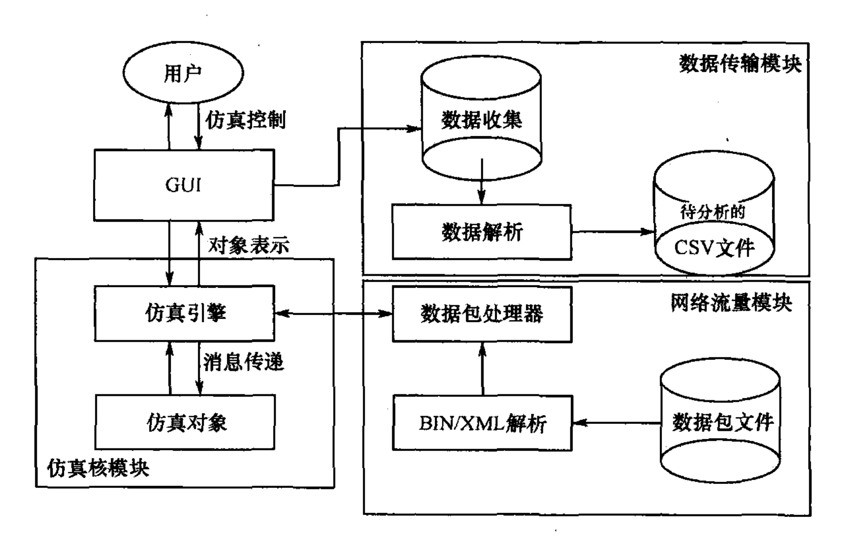


图 17.5　WINDS 体系结构

SEMU 也是一种基于 Linux 操作系统的模拟器，在模拟过程中将实际节点和用软件模拟的虚拟节点相结合，采用类似于 TOSSIM 的静态翻译技术，能直接对实际节点中的代码进行仿真，这些代码可在实际节点上运行。SEMU 通过对实际节点构成的网络及虚拟网络同时协仿真，提高纯软件仿真的精度。SEMU 仿真原理如图 17.6 所示。

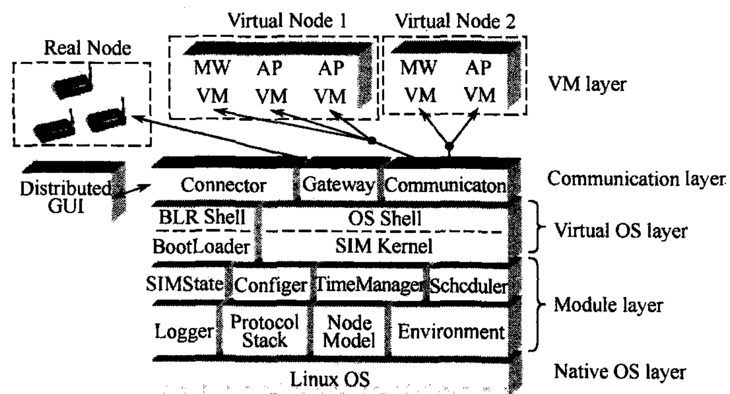


图 17.6　SEMU 结构图

EmStar 是基于 Linux 操作系统，用于仿真分布式系统的平台，并可用真实的物理信道代替模拟信道。它支持异构网络的仿真和模拟，网关节点采用 Crossbow®的 Stargate，也称为微服务器节点。微服务器节点采用 X - Scale 处理器，运行 Linux 操作系统，可作为网关节点，同时也可外接普通节点 Mica2，一方面可以在普通节点的基础上再进行更多的计算处理，另一方面也可以使微服务器节点利用 Mica2 的通信信道。

此外，还有 J - Sim、ESyPS 等模拟器，它们的系统结构和节点结构如图 17.7 ~ 图 17.12 所示。

17.1.3　无线传感器网络后台软件

国内外已经开发出了几种无线传感器网络监控平台的后台软件，如中国科学院计算

所的 SNAMP[7]，美国 Crossbow 公司的 Surge Network Viewer、TinyViz 和 MOTE - VIEW[8]，德国 Lubeck 大学的 SpyGlass[9]等。

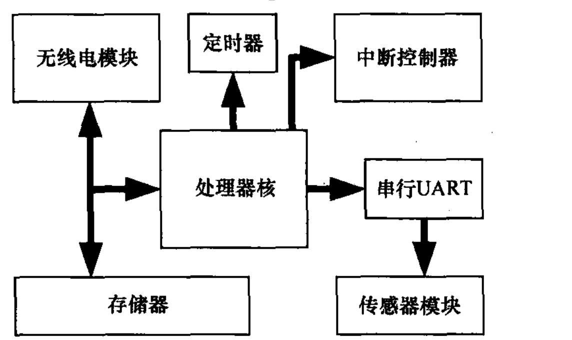


图 17.7 ESyPS 模拟器结构图

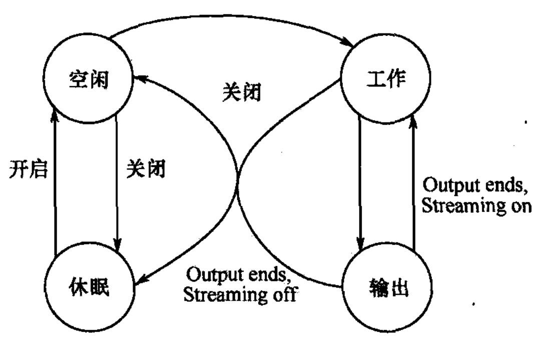


图 17.8 ESyPS 模拟器传感节点状态机

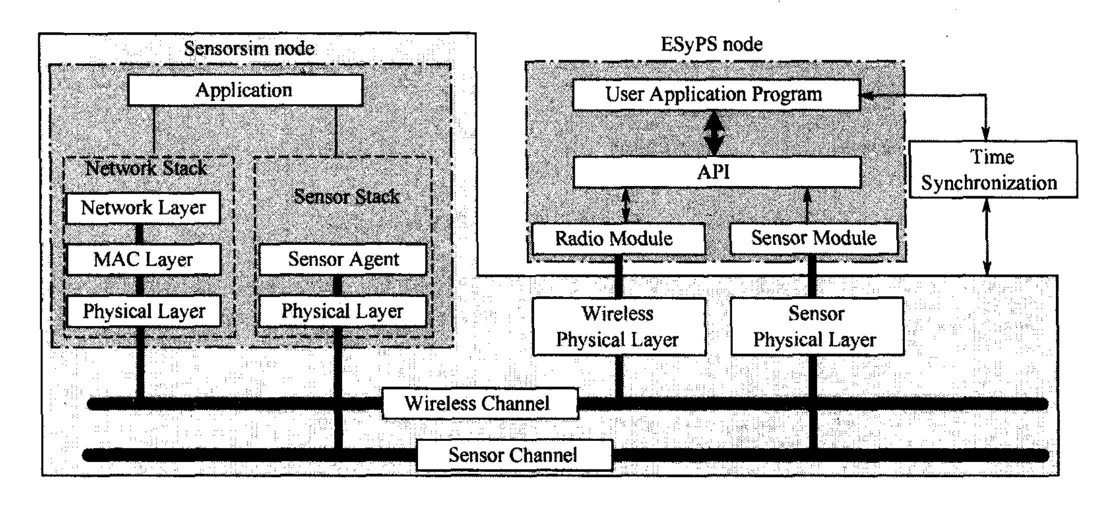


图 17.9 联合仿真框架中的节点结构

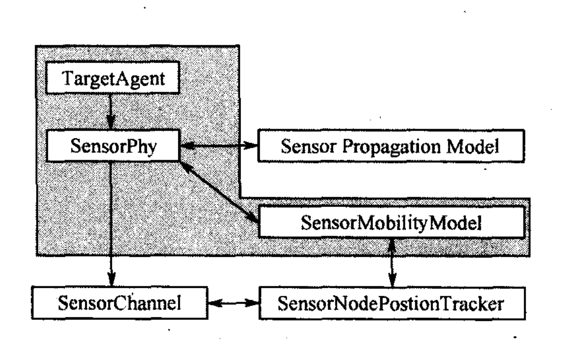


图 17.10 ESyPS 模拟器无线电模型

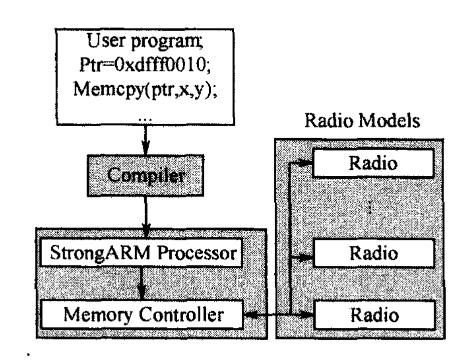


图 17.11 J - Sim 模拟器目标节点与其他组件关系图

SNAMP 由 3 个主要部分组成，即传感器网络、数据收集网络和可视化服务器。传感器网络由 GAINS - 4a 节点组成，数据收集网络由 GAINS - 3 节点组成，可视化服务器包括串口监听模块、MAC 层分析模块、网络层分析模块、传感数据分析模块、数据库管理模块以及数据处理模块等。模块化的设计，使得整个系统层次清晰，可扩展性良好。同时，

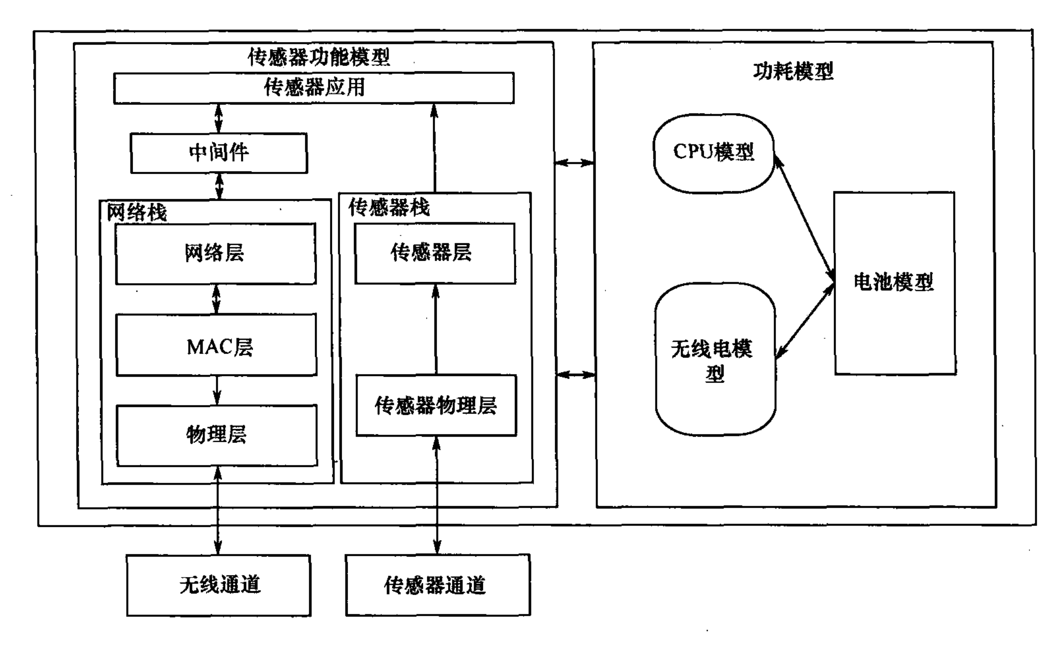


图 17.12　J-Sim 模拟器传感节点内部结构

SNAMP 提供了多种形式的用户接口，包括拓扑树、节点分布、实时曲线、数据查询以及节点列表等，满足用户在应用无线传感器网络时的种种需求，软件总体结构如图 17.13 所示。

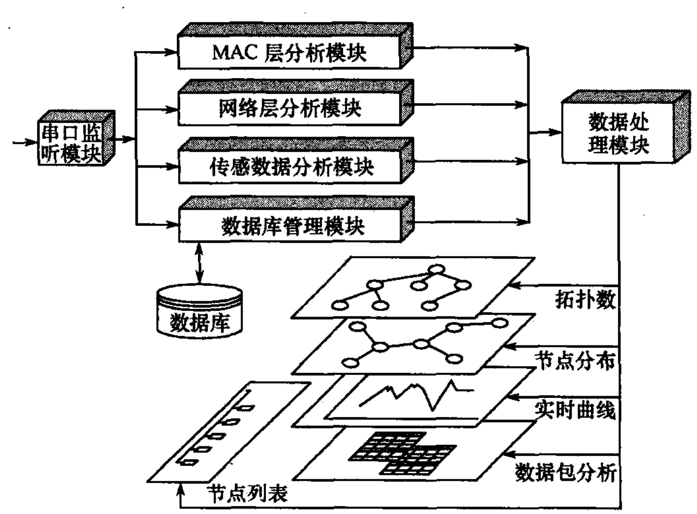


图 17.13　SNAMP 的总体结构

Surge Network Viewer 和 MOTE-VIEW 是 Crossbow 公司用来可视化显示无线传感器网络的产品。Surge Network Viewer 仅有的功能是可视化网络的拓扑结构，网络状态的记录和显示，诸如节点的出现、预测和连接状态等。MOTE-VIEW 除了包括 Surge Network Viewer 的功能以外，有更清晰的用户接口和更多的功能，能够将传感器的数据记录到数据库中，并进行分析，绘制出传感器数据的曲线和节点的拓扑结构，如图 17.14 所示。它允

许以类似于数据库的形式收集数据来查询传感器网络。MOTE - VIEW 利用网关(Sink)从传感器网络中收集数据。

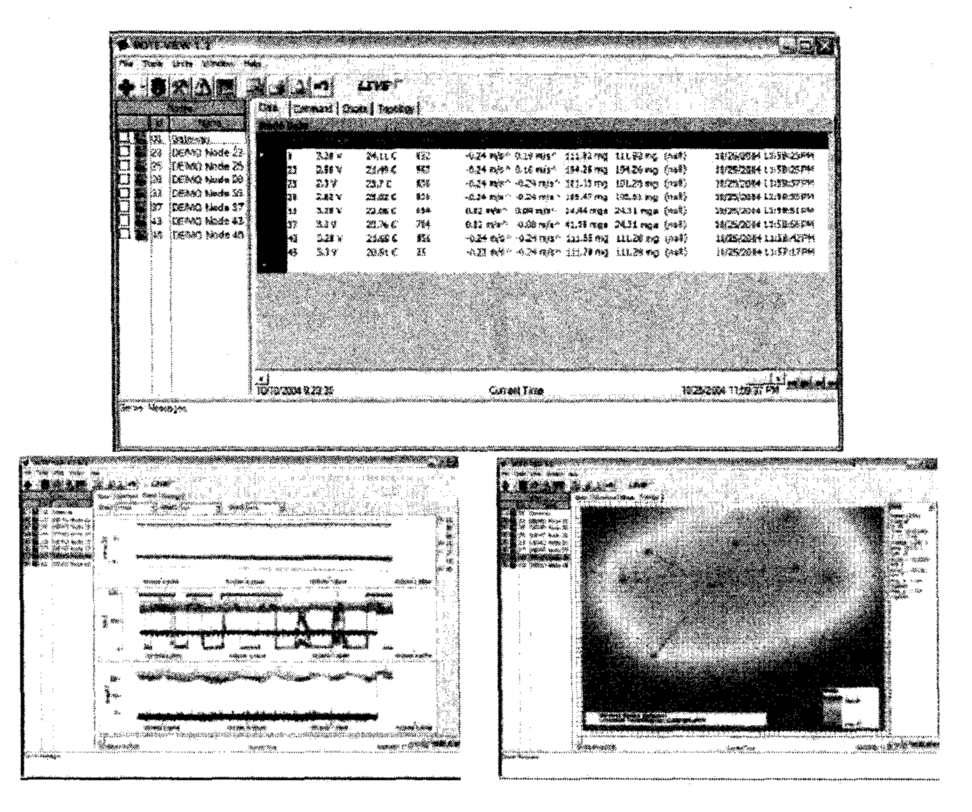


图 17.14　MOTE - VIEW 可视化界面

TinyViz 是 TinyOS 操作系统 TOSSIM 包的一部分。它能够可视化传感器读数、LED 的状态、无线通信连接和与运行中的 TOSSIM 仿真器交互。TinyViz 的结构允许增加特定的可视化功能,包括为特定事件的绘图操作、确认、反应和为 TOSSIM 仿真器提供反馈。TinyViz 与 TinyOS 操作系统、TOSSIM 仿真器和 Mica 系列无线传感器网络硬件节点共同使用。

SpyGlass 是一个应用于无线传感器网络的模块化和可扩展的可视化架构。SpyGlass 利用一个多层的结构来显示无线传感器网络的信息,可以根据特定的需求和应用来增加新的可视化模块。SpyGlass 的图形显示界面包括背景层、连接层和节点层。背景层用来绘制可视化界面的背景,连接层显示节点间所有的连接关系,节点层显示实际的节点。每一层均由相应的模块来实现。除了以上 3 个模块以外,还有另外两个模块,即节点定位模块和全局信息模块。节点定位模块由其他模块调用来决定在界面的什么位置放置节点和绘制节点间的连接。全局信息模块以文本的方式显示部分或全局网络的信息,总体结构如图 17.15 所示。在 SpyGlass 中,单个节点发出数据,由一个网关来收集数据,通过 TCP/IP 传送到远程计算机上的可视化软件中。

此外,具有类似功能的后台软件还有美国 Daintree Networks 公司的 SENSOR NETWORK ANALYZER[11] 和 Ember 公司的 Ember StudioNetwork Management Software 等。

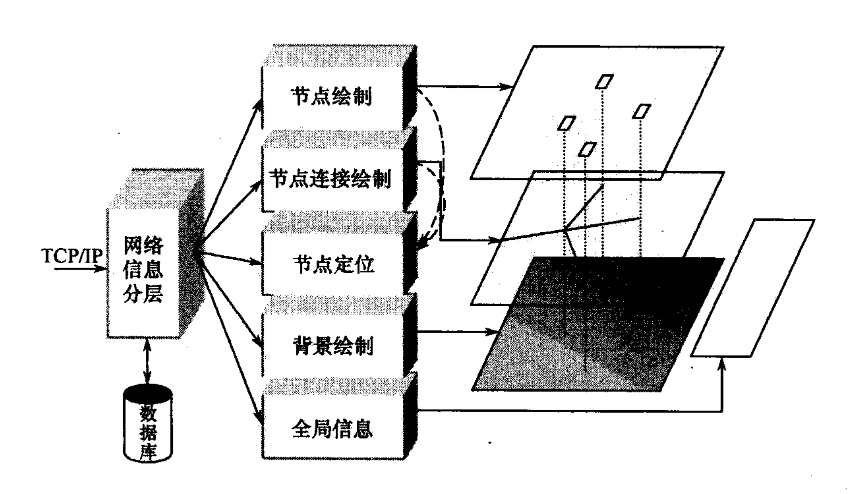


图 17.15　SpyGlass 总体结构

17.2　分簇型无线传感器网络模拟器 CWSNS 的设计与实现

从对现有无线网络模拟器的概述来看，现有的无线网络模拟器大都以地址和数据传输为中心，强调通信协议和通信链路，不关心具体的感知数据特征和应用类型，也未考虑节点能量受限问题。而现有的无线传感器网络模拟器，虽然在设计过程中考虑了无线传感器网络的特点，并将节点模型、能耗模型等加入模拟器中，但这些模拟器大都基于 Linux 平台开发，编译过程复杂，且仿真结果的可视化和人机交互性一般。

本节利用 OOP 技术，以 C + + Builder 为开发环境，将节点分布模型、电池放电模型、节点能耗模型、流量模型、路由协议和 MAC 协议等以类的形式进行封装，构成面向对象的网络模拟器。并利用 C + + Builder 丰富的图形控件，以曲线和表格的形式实现了无线传感器网络模拟结果的形象化输出。本节设计的模拟器 CWSNS，主要用来进行分簇型无线传感器网络 MAC 协议和路由协议的仿真。

由于采用 OOP 设计思想，可在不改变模拟器结构的基础上方便地添加和修改各个模型，使得模拟器易于扩展和升级。

17.2.1　CWSNS 的结构与原理

在设计模拟器时，遵循整体性、高效性、扩展性和面向应用性等原则。据此，使用主流的面向对象程序设计语言 C + + Builder 设计 CWSNS。采用 C + + Builder 开发环境，一方面 C + + Builder 是基于 C + + 的支持面向对象程序设计；另一方面，C + + Builder 对 API 函数进行封装，形成了非常丰富的控件，便于为用户提供良好的人机交互能力。

CWSNS 原理结构如图 17.16 所示。在网络仿真系统中需要建立的模型主要有电池放电模型、能耗模型、拓扑模型、流量模型、协议模型。本文设计的 CWSNS 网络模拟器包含这 5 种基本模型。

在图 17.16 所示的原理结构图中，各组件的功能如下：

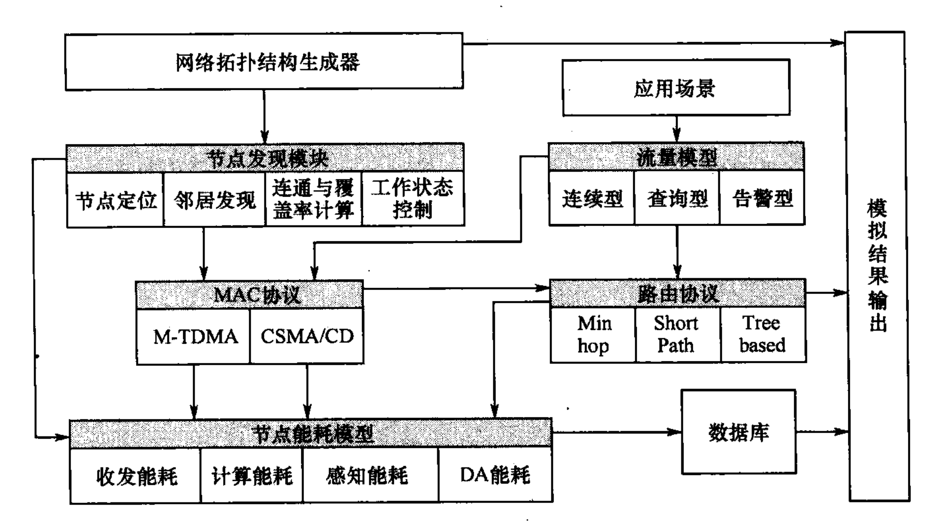


图 17.16　模拟器原理结构图

(1)网络拓扑结构生成器。根据输入的参数生成所需的网络拓扑结构,包括节点数目、节点布置策略(随机部署、网格部署)、区域大小、Sink 的位置、节点通信半径、节点感知半径。

(2)节点发现模块。节点根据网络拓扑结构确定自身的位置,发现通信范围内的节点;并根据网络连通与覆盖度要求控制节点的工作状态。

(3)流量模型。模拟不同应用类型的流量,包括泊松流量、随机流量和均匀流量等。典型的流量数据存储在 Access 数据库文件中;在仿真过程中,通过调用数据库的形式产生流量。

(4)MAC 协议。提供几种基本 MAC 协议,如 TDMA、S - MAC、TRAMA、CSMA/CD 及本文研究的 M - TDMA,为上层协议的仿真提供支撑;也可以根据网络拓扑结构、流量分布、节点位置,设计新的 MAC 协议。

(5)路由协议。在 MAC 协议的支持下,根据节点位置、链路质量模拟单源单汇及多源单汇路由协议。

(6)节点能耗模型。模拟实际节点的数据采集、数据聚集和无线收发的能耗;考虑到节点剩余能量与电池放电特性有关,在节点能耗模型组件中,包含了电池放电模型。

(7)数据库。用于保存节点位置、节点剩余能量、节点路由表等参数;同时保存仿真结果,便于以后分析。

(8)模拟结果输出模块。以图形和表格的形式输出模拟结果。

17.2.2　典型类的设计

类的设计是 CWSNS 的基础,也是模拟器扩展性的体现。通过添加或修改类的方式,可扩展模拟器的功能。现有类的定义及功能如下。

1. 拓扑结构类

拓扑结构类实现节点布置、包括节点数目、区域边长和布置方式,其定义如表 17.1 所列。

表 17.1 拓扑结构类设计

```
class Topology
  {
    int NodeNumber;                                              // 节点数目
    int length;                                                  // 区域半径
    float RandomDistribution(int NodeNumber, int length);        // 节点随机分布
    float GaussianDistribution(int NodeNumber, int length);      // 高斯分布
    float GridDistribution(int NodeNumber, int length);          // 网格分布
  };
```

2. 节点类

节点类的定义如表 17.2 所列。

表 17.2 节点类设计

```
class Node
  {
    int ID;                        // ID 号
    float x,y;                     // 坐标
    float ComRadius;               // 通信半径
    float SensRadius;              // 感知半径
    float ResidualEnergy;          // 剩余能量
    bool NodeType;                 // 节点类型:true 为成员节点;false 为簇头
    float DischargeMode(void);     // 电池放电模型
    float TransmitEnergy(float Distance, int MessageLength);   // 发送能耗
    float ReceiveEnergy(float Distance, int MessageLength);    // 接收能耗
    float DataAggregation(int len);    // 数据聚集能耗
  };
```

在节点类中,利用节点地理位置作为标识给节点命名,避免用 IP 地址命名时开销大的问题。

节点类的成员方法 DischargeMode( )提供以下两种电池模型:

(1)线性模型,即

$$C_r = C_{t_0} - \int_{t_0}^{t_0+t_d} I(t)\,\mathrm{d}t \tag{17.1}$$

式中:C_r 为剩余容量;C_{t_0} 为 t_0 时刻的剩余容量;$I(t)$ 为放电电流。

(2)放电速率相关模型。在线性模型中,假设电池的最大容量不受放电速率的影响。已有研究表明,电池的容量受放电速率的影响。引入电池容量因子 $k = C_{eff}/C_{max}$,其中,C_{eff} 为有效容量,C_{max} 为最大容量。因此

$$C_r = kC_{t_0} - \int_{t_0}^{t_0+t_d} I(t)\,dt \tag{17.2}$$

并且,负载越大,C_{eff} 越小,k 值也越小;负载越小,C_{eff} 越大,k 值亦增大。

电池放电过程是个复杂的过程,较为精确的放电模型与电极、电解液的种类有关。文

献[10]指出，电池的放电特性受 50 多种物理和化学参数的影响。可结合实际节点的放电特性曲线，拟和出放电模型。

节点类的成员方法 TransmitEnergy( )根据节点和簇头的距离 d 与阈值距离 d_0 的关系，发送能耗模型包括自由空间发送方式和多通路衰减方式。

关于能耗模型中的参数，如 E_{elec}、k 和 ε_{fs} 等，有些模拟器以对实际节点的测量结果作为能耗模型参数，精度较高，但通用性不强。

3. 流量类与 MAC 协议类

流量类的定义如表 17.3 所列。

CWSNS 模拟器提供两种类型的流量，由 TrafficMode Type 的赋值决定。特征流量数据事先保存在 Access 数据库中，开始仿真后，根据仿真周期从数据库中读出流量值。

MAC 协议类的定义如表 17.4 所列。

表 17.3　节点流量类设计

```
class TrafficMode
  {
    int TrafficMode Type; // 1 为泊松流量,2 为均匀流量
  };
```

表 17.4　MAC 协议类的设计

```
class MAC
  {
    NodeToCH( );  // 簇内 MAC 协议
    CHToSink( );  // 簇间 MAC 协议
  };
```

MAC 类负责无线信道的模拟，包括信道的建立、维护和控制，减少邻节点广播引起的冲突。目前，模拟器提供两种信道接入方法，节点和簇头之间采用 TDMA、M - TDMA 方式通信，每个节点在相应的时间隙内向簇头发送数据包，避免数据包的冲突；簇头和 Sink 之间采用具有碰撞监测的 CSMA/CD 方式通信。如果两个簇头同时进行发送，就会监测到碰撞并停止发送。

4. 路由协议类

路由协议类的定义如表 17.5 所列。

表 17.5　路由协议类的设计

```
class routing
  {
    bool CHSelection(int ID, float Residual Energy, float x, float y);
    PMRP (float source x, float source y, float sink x, float sink y);
    DLBTP(float sink x, float sink y)
  };
```

该类中只包含 3 个成员方法 CHSelection( )，节点布撒后周期性地将剩余能量、距离 Sink 节点的距离和节点通信半径等参数发送至 Sink 节点。Sink 节点根据方法 CHSelection( )运用模糊推理方法，决定哪些节点担当簇头，并将该决定广播给区域内的节点。节点收到 Sink 节点的广播信息后，将感知数据发送至自己对应的簇头，簇头完成本簇数据的聚集和向 Sink 节点的发送。PMRP( )根据源簇头和 Sink 节点的位置，执行基于优先级

的多径路由算法。DLBTP( )则根据 Sink 节点位置，在所有簇头和 Sink 节点之间建立负载均衡路由树。

17.2.3　类的相互关系

除了上述几种典型的类外，模拟器还包括离散事件类 DisEvent、事件列表类 EventList、事件序列类 EventQueue 及模拟结果输出类 Result 等，这些类的相互关系如图 17.17 所示。可以结合具体的仿真需要，在这些类的基础上添加新的类。

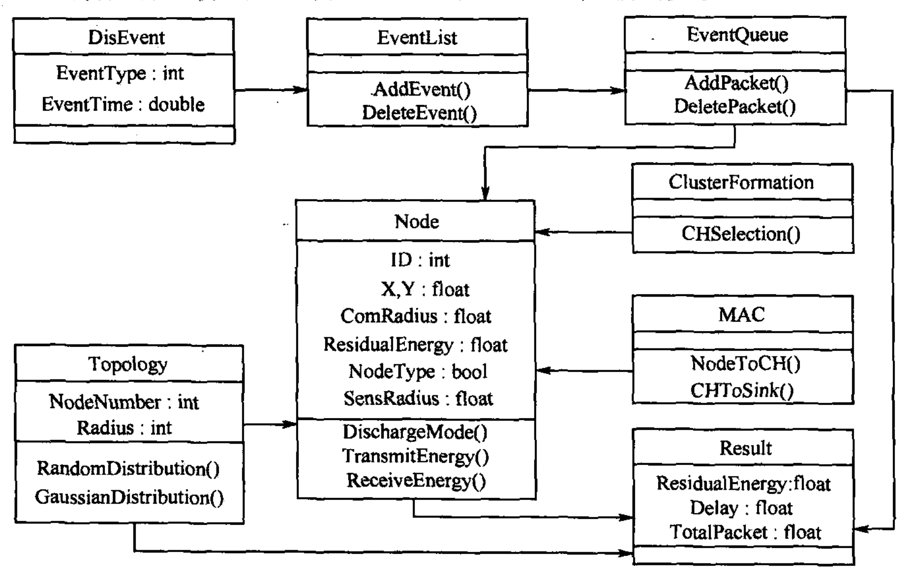


图 17.17　类的相互关系总图

17.3　CWSNS 仿真流程及仿真实例

根据模拟网络协议层次的不同，仿真流程相应变化。下面以对路由协议的仿真为例，描述 CWSN 仿真流程。

17.3.1　CWSNS 仿真流程

模拟过程如图 17.18 所示：在初始化阶段设置节点位置、Sink 节点位置、节点数和监测区域的大小、通信半径、感知半径。这个过程也可通过读取存储在 PC 硬盘上的 Access 数据库完成，便于重复实验相同网络拓扑结构采用不同协议的性能。

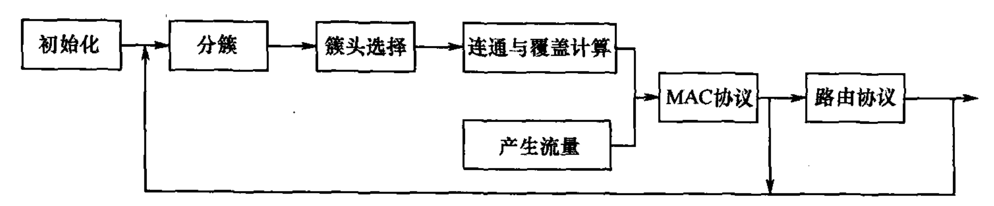


图 17.18　模拟器仿真流程

模拟器读取 Access 数据库中的节点位置的代码如表 17.6 所列，模拟节点产生流量

时，也可通过类似代码读取数据库中的典型流量值。

初始化完毕后即可运行模拟器自带的模糊 C 均值聚类的分簇算法或 LEACH 算法，也可基于节点类和拓扑结构类设计新的分簇算法。经过簇头选择阶段后，根据通信半径和感知半径设置节点工作状态，并结合流量类型选择 MAC 协议。若要重新设计 MAC 协议，或只对 MAC 协议进行仿真，可调用现有的类进行设计。

路由协议仿真阶段需要分簇算法、MAC 协议、拓扑结构等支持，是 CWSNS 所能仿真的最高层次的网络协议。

表 17.6　模拟器读取 Access 数据库中的节点位置的代码

```
void __fastcall TCoForm::FormCreate(TObject * Sender)
{
   AnsiString cns;
   cns = "Provider = Microsoft. Jet. OLEDB. 4. 0;Data Source = "
        + ExtractFilePath(Application - > ExeName)
        + "coordination. mdb;Persist Security Info = False;Jet OLEDB:Database Password = XXX";
   ADOQuery1 - > ConnectionString = cns;    // 指定 Access 数据库路径,XXX 为数据库密码
   AnsiString sql_1;
   sql_1 = "select * from coordination";
   ADOQuery1 - > Close();
   ADOQuery1 - > SQL - > Clear();
   ADOQuery1 - > SQL - > Add(sql_1);         // 读取节点位置
   ADOQuery1 - > Open();
}
```

在仿真过程中，可查询某个节点、簇头和网络总能耗，也可监测网络拓扑结构和路由树或路由路径。当模拟时间达到设定值或网络失效时，退出仿真过程。

17.3.2　仿真实例

本节通过对基于动态负载均衡树 DLBTP 路由协议的仿真，说明 CWSNS 模拟器的工作过程。运行模拟器的计算机主要配置为 CPU Intel Centrino Duo 1.66GHz × 2；RAM 512M；操作系统 Windows XP®。

CWSNS 主界面如图 17.19 所示，主界面分为仿真结果显示区、仿真参数设置区和消息报告区。其中，仿真结果显示区包括拓扑结构、能耗曲线、分簇结构、路由树结构和丢包数目 5 个子显示。

在仿真过程中，可查看相应参数的变化。设置与网络拓扑结构相关参数后，即可获得节点在区域中的初始拓扑结构图。

图 17.20 是 100 个节点按照随机布置的方式在监测区域中的初始位置，Sink 节点的位置为(170，300)。运用本书提出的基于模糊 C 均值聚类的分簇算法对节点进行分簇，结果如图 17.21 所示。

在“节点流量类型”中选择需要的类型，如随机流量。这样，成员节点就可以在每轮中向簇头发送感知数据。结合 MAC 协议，可统计丢包率和吞吐量等参数。

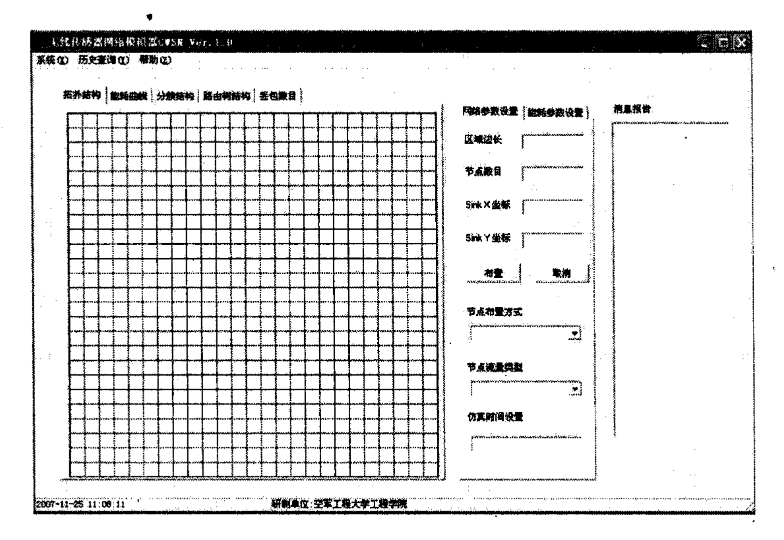


图 17.19　CWSNS 主界面

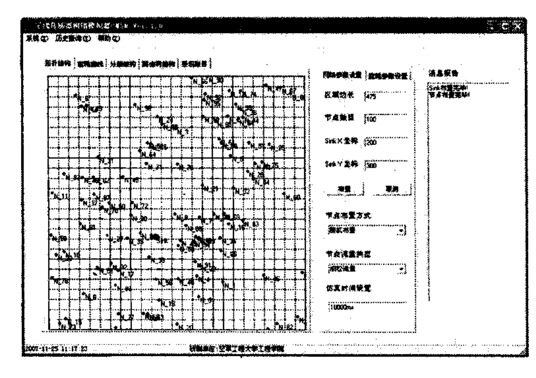


图 17.20　网络初始拓扑结构

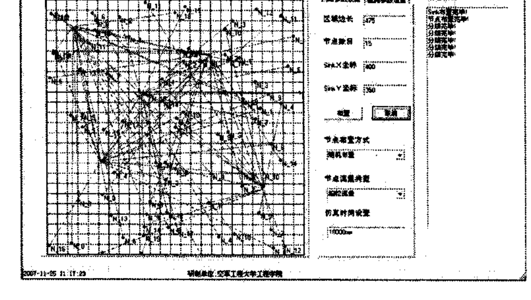


图 17.21　分簇结构图

DLBTP 路由协议的代码已事先编写好,通过调用节点类、流量和 MAC 协议等类,结合能耗模型,可得如图 17.22 所示的动态负载均衡树结构。图 17.23 是选择不同 MAC 协议时的总丢包率曲线图。

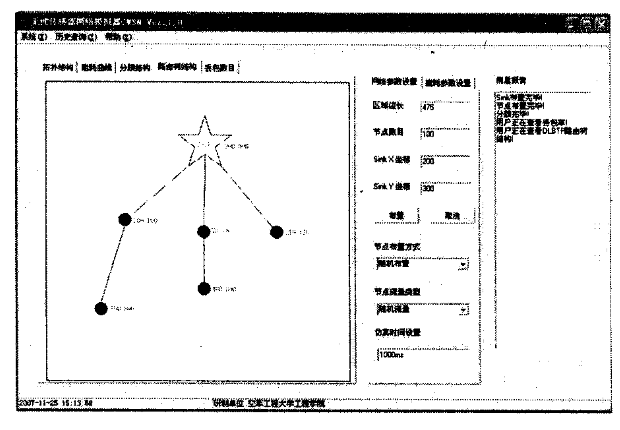


图 17.22　路由树结构

若需要验证其他 MAC 或路由协议的性能,CWSNS 模拟器可以提供基础类供调用和

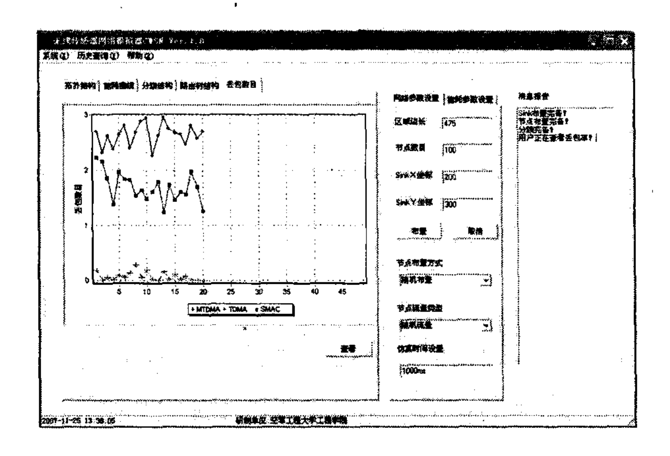


图 17.23 不同 MAC 协议时的总丢包率曲线图

修改。用户也可对新的协议进行封装,体现了 CWSNS 模拟器具有一定扩展性。

从对现有无线网络模拟器的概述来看,现有的无线网络模拟器大都以地址和数据传输为中心,强调通信协议和通信链路,不关心具体的感知数据特征和应用类型,也未考虑节点能量受限问题。现有的无线传感器网络模拟器,虽然在设计过程中考虑了无线传感器网络的特点,并将节点模型、能耗模型等加入模拟器中,但这些模拟器大都基于 Linux 平台开发,编译过程复杂,且仿真结果的可视化和人机交互性一般。

因此,有必要研究符合无线传感器网络特点、编译和配置简单、提供良好的人机交互能力的网络模拟器。

参考文献

[1] NS-2: Network Simulator-2 [EB/OL]. http://www.isi.edu/nsnam/ns, 2004.

[2] SensorSim[EB/OL]. http://nesl.ee.ucla.edu/projects/sensorsim/,2005.

[3] Takai M, Bajaj L, Ahuja R. GloMoSim: A Scalable Network Simulation Environment[R]. UCLA, Computer Science Department, 1999.

[4] 石怀伟, 李明生, 王少华. 网络仿真技术与 OPNET 应用实践[J]. 计算机系统应用, 2006,3:49-55.

[5] SENSE: Sensor Network Simulator and Emulator [EB/OL]. http://www.cs.rpi.edu/cheng3/sen-se.2004.

[6] Levis P, Lee N, Welsh M, etc. TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications [A]. Proceedings of SenSys04[C]. 2004: 1882-2002.

[7] Shawn: The Swarm Net project [EB/OL]. http://www.swarmnet.de, 2005.

[8] Heemin Park, Weiping Liao, King Ho Tam, etc. A Unified Network and Node Level Simulation Framework for Wireless Sensor Networks[R]. TR-UCLA-NESL-170309-02, NESL Technical Report, September, 2003.

[9] Ratan K. Guha, Oleg Kachirski. An Architecture for Distributed Simulation of Wireless Networks[A]. Proceedings of 18th European Simulation Multi conference[C]. Graham Horton, Europe, 2004.

[10] Girod L, Elson J, Cerpa A, etc. EmStar: a software environment for developing and deploying wireless sensor networks [A]. Proceedings of the USENIX Technical Conference[C]. 2004.

[11] Shih-Hsiang Lo, Jiun-Hung Ding, Sheng-Je Hung. SEMU: A Framework of Simulation Environment for Wireless Sensor Networks with Co-simulation Model[A]. Proceedings of the 5th International Conference on Embedded Networked Sensor Systems[C]. Sydney Australia, 2007: 275-288.

第 18 章　无线传感器网络应用实例

无线传感器网络的研究直接推动了以网络技术为核心的新军事技术革命，并诞生了网络中心战的思想和体系，催生了 C^4ISRT(Command, Control, Communication, Computing, Intelligence, Surveillance, Reconnaissance, Targeting)系统等重要军事思想和体系。C^4ISRT 系统的目标是利用先进的高科技技术，为未来的现代化战争设计一个集命令、控制、通信、计算、智能、监视、侦察和定位于一体的战场指挥系统，受到了军事发达国家的普遍重视。

18.1　军事应用

因为传感器网络是由密集型、低成本、随机分布的节点组成的，自组织性和容错能力使其不会因为某些节点在恶意攻击中的损坏而导致整个系统的崩溃，这一点是传统的传感器技术所无法比拟的。也正是这一点，使传感器网络非常适合应用于恶劣的战场环境中，包括监控我军兵力、装备和物资，监视冲突区，侦察敌方地形和布防，定位攻击目标，评估损失，侦察和探测核、生物和化学攻击等。

(1)监控我军兵力、装备和物资。指挥官可以实时地监控我方部队的状况，在战场上通过传感器网络监控我军装备和物资的状态和可用性。在每个部队、车辆、装备和关键物资上安装传感器，这些传感器可以报告相应的状态。所有这些数据通过汇聚节点最终发送给终端的指挥官，最后融合来自各战场的数据后再将数据发送到更高层的指挥官。

(2)战场监控。对关键的区域、可通过的路线，可以快速地部署传感器来严密监控这些军事要地的各种情况。随着监控方法的发展和新方案的提出，新型传感器网络可以随时部署到军事要地。

(3)侦察敌方兵力部署和地形。传感器网络可以部署在敌军前线，以更隐蔽的方式近距离地观察敌方的布防；也可以直接将传感器节点撒向敌方阵地，在敌方还未来得及反应时迅速收集利于作战的信息。

(4)目标定位。传感器网络可以嵌入导航系统，来提供精确的定位信息。

(5)侦察和探测核、生物和化学攻击。在化学和生物战中，在爆炸中心附近及时、准确地采集数据非常重要，传感器网络可以部署在我军前沿，作为化学和生物攻击的预警系统，这样就可以为我军提供宝贵的反应时间，大幅度降低人员伤亡。传感器网络也可以在核、生物和化学攻击后提供精确的探测数据，我们可以部署传感器网络来探测数据从而避免核反应部队探测数据时受到核辐射。

在战场，指挥员往往需要及时准确地了解部队、武器装备和军用物资供给的情况，铺设的传感器将采集相应的信息，并通过汇聚节点将数据送至指挥所，再转发到指挥部，最

后融合来自各战场的数据形成我军完备的战区态势图。在战争中，对冲突区和军事要地的监视也是至关重要。当然，也可以直接将传感器节点撒向敌方阵地，在敌方还未来得及反应时迅速收集利于作战的信息。传感器网络也可以为火控和制导系统提供准确的目标定位信息。在生物和化学战中，利用传感器网络及时、准确地探测爆炸中心将会为我军提供宝贵的反应时间，从而最大可能地减小伤亡。传感器网络也可避免核反应部队直接暴露在核辐射的环境中。

【应用实例 18.1】单兵作战系统应用方案

单兵综合作战系统如图 18.1 所示，是以单兵为基本单元，人机环境统筹考虑，应用多种先进技术的高技术士兵装备系统，使士兵、武器、装备间形成了一个有机的整体，从而全面增强单兵的火力、机动、通信、观瞄和防护能力，使每一个士兵都成为有效的火力攻击单位，既能独立作战，又能协调行动，全面提高单兵作战效能，使士兵有条件在未来信息化战场上赢得优势。

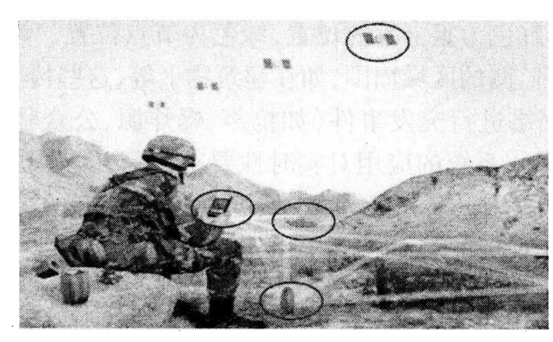


图 18.1　单兵作战系统示意图

单兵综合作战系统一般分为 5 个子系统，即武器子系统、通信子系统、观瞄子系统、生命子系统、防护子系统。

其中，通信子系统主要是提高单兵的全天候作战能力及单兵之间、分队之间、单兵与后方指挥员之间的联系及情报交换能力，包括分队内部成员之间短距离通信设备以及分队与后方指挥员之间长距离通信设备。

生命子系统主要是利用各种传感器对士兵各种生命体征以及周围环境数据进行采集分析，由单兵穿戴式计算机对传感器的监测结果进行分析，得出一个数值代码并将其发送到后方指挥部，指挥员就可判断出前线作战士兵的生理状态：是否受伤，伤情如何；是否处于疲劳、寒冷、疾病、恐惧等不良状态等。这对伤病员的及时救护、给养的供应提供了客观依据，并使指挥员对部队的战斗力有一个准确的判断。ZigBee 短距离、低成本、低功耗、易实现的特点非常适合作为生命子系统的组成部件。

在一个单兵小分队中，每个分队成员佩戴一个 ZigBee 生物传感器节点。该节点是集 ZigBee 无线网络模块与生物传感器模块为一体的，可以对士兵生命体征诸如脉搏、血压、呼吸、体温等进行数据采集，并通过 ZigBee 方式无线传输至主协调器，主要由脉搏传感器、温度传感器、状态传感器、模拟信号放大器、A/D 转换器、电平比较器、信号存储器和 ZigBee 无线收发器及相关软件组成。

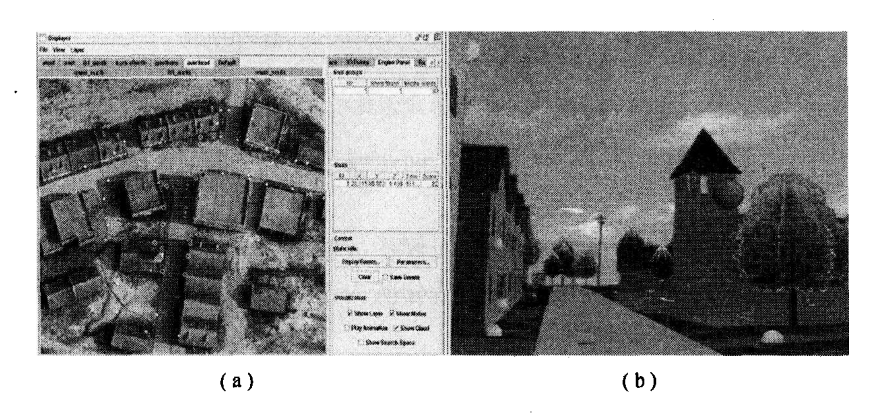
位于小分队中心位置的成员身上携带有 ZigBee 主协调器。主协调器的主要功能是为建立和启动网络这一过程设置参数，其中包括选择一个射频信道、唯一的网络标

识符以及一系列操作参数。每个 ZigBee 网络都必须包括一台主协调器，在本应用中，由于小分队成员的活动范围非常接近，所以无需中继设备，可以直接将终端无线接入主协调器。

ZigBee 所具有的短距离、低成本、低功耗、易实现、安全可靠的特点非常适合作为单兵作战系统中生命子系统的组成部件。不仅能对士兵生命体征数据进行传输，后续的技术开发还可以对敌核、生、化武器污染监测数据进行传输。当传感器的检测信号表明敌方施放了核、生、化武器，就会自动发出报警信号，同时将检测结果通过 ZigBee 发送装置传输到指挥部，为己方赢得较长的预警时间。ZigBee 的应用为指挥人员提供了准确评价部队战斗力的客观依据，提高了部队装备的信息化含量，可以使我军在未来信息化战争中处于有利地位。

【应用实例 18.2】美国军方枪声定位系统应用方案

2005 年，美国军方成功测试了由美国 Crossbow 公司的产品 MICA2 组建的枪声定位系统。如图 18.2 所示，红色为狙击手的位置，绿色为节点位置。该方案是通过把众多的传感器节点安置在所要监测的区域周围，如在建筑物上等，这些传感器节点能够有效地按照一定的程序组建成网络进行突发事件（如枪声、爆炸源、公众骚扰地等）的检测，为救护、反恐等提供有力手段。系统的应用对实时性要求很高，因而方案中主要的器件是 60 个 MICA2 传感器节点及定制的传感器模板，经过鉴定，确定该方案试验时的检测精度可达到 1m，反应时间小于 3s，这些指标达到了预先的要求。



(a)　　　　　　　　(b)

图 18.2　狙击手定位系统与检测区域俯瞰图

(a)狙击手定位系统；(b)检测区域俯瞰图。

该系统中还用到地理信息技术和定位技术，对于检测到的位置（枪声、爆炸源等）通过系统中的软件系统，并且借助显示系统把位置的具体地址方位等在电子地图上标示出来，指挥中心可以根据这些信息，迅速进行事件发生后的救护等方案的确定，从而能够及时赶到事发现场，这样也有利于对事件进行侦查破案。

该系统的原理很有推广性。由于该系统的成功试验，不但在美国军方引起了极高的重视，而且美国的公安警察等部门也对该技术感兴趣。公安部门把该系统应用到枪声等突发事件发生率比较高的公共场所，这对及时处理突发事件起到了重要作用。该方案虽然没有得到真正的应用，但是基于实用性和国家军方、安全、公安等部门机构的技术需求方面综合分析，该方案终将会投入到实际应用中去。

18.2　国家安全

无线传感器网络作为一种新兴的检测技术，具有快速布置、自组织等特性，胜任大范围、多信号的分布式检测，可以在安全预警、应急处理和灾后恢复等安全措施中发挥重要的作用。

【应用实例 18.3】面向 2010 年上海世博会安全保障的无线传感器网络系统

2010 年上海世博会是继 2008 年北京奥运会后的中国人民的又一盛事。据预测，此次世博会的参加人数将超过 5000 万人次，上海旅游业的直接收入将达 91.1 亿元人民币，其后继经济影响更是无法估量。而且，上海位于长江之首，世博会的举办必将产生显著的周边联动效应，带动华东，甚至辐射全国，对社会经济文化的发展具有不可低估的影响力。因此，为了保证此次上海世博会的胜利召开，必须确保世博会期间各方面的安全，特别是水、电、煤气、交通等重要基础设施和会展场馆等重要场所的安全。必要的安全措施包括安全预警、应急处理和灾后恢复等，把此次世博会真正举办成中国人民的一大盛事。

中国近年来经济的高速发展和上海的明星城市地位，将会吸引大量的参展国家、国际组织和参观人员。此次世博会跨越浦江，规划范围为 5.28km^2，其场馆总建筑面积达 80 万 m^2，是目前亚洲最大的展馆。另外，近年来各种恐怖活动极其猖獗，极大地影响了世界的和平发展。这些因素对于上海世博会的安全保障都将是极大的挑战。为了迎接这些挑战，单纯增加人力是远远不够的，必须借助各种高科技手段来保证此次世博会的安全顺利进行。而能够胜任大范围、多信号的分布式检测的无线传感器网络（Wireless Sensor Networks，WSN）便是我们可以倚重的安全辅助技术之一。

为了保证 2010 年世博会的安全顺利进行，应当制定包括安全预警、应急处理和灾后恢复等必要的安全机制，并借助 WSN 等信息技术手段来确保这些安全机制能够快速有效运行。在安全保障中，WSN 主要负责提供环境检测信息，作为安全机制的决策依据。下面列举了 WSN 在 2010 年上海世博会安全应用中的 3 个典型场景，分别对应于安全预警、应急处理和灾后恢复等安全机制。

在 2010 年世博会的安全保障中，无线传感器网络主要用于在一些重要设施和场所对爆炸物、有毒气体等目标的静态和动态检测，其应用过程一般如下所述：

（1）根据待检测目标和预期应用环境，设计和开发集成了相关传感器的节点。

（2）将这些传感器节点布置在检测区域，经过简单的初始化配置，这些节点组网形成无线传感器网络，并准备接受检测任务。

（3）根据控制台的命令完成有关检测任务，并定期汇报或紧急报告检测信息至控制台，供安全预警、应急处理和灾后恢复等机制决策参考。

18.3　工业领域

18.3.1　工业安全

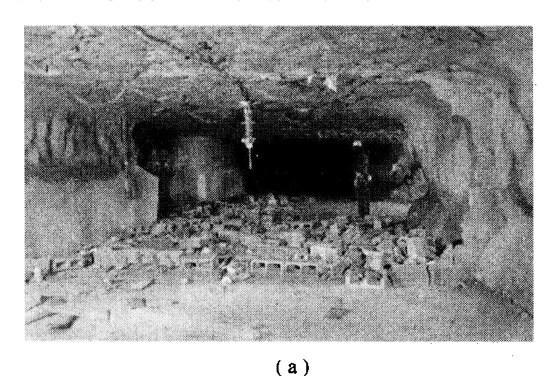
无线传感器网络可用于各种危险工作环境，如在煤矿、石油钻井、核电厂和组装线工

作的员工将可以得到随时监控。这些传感器网络可以告诉工作现场有哪些员工、他们在做什么，以及他们的安全保障等重要信息。在相关的工厂每个排放口安装相应的无线节点，完成对工厂废水、废气污染元的监测，样本的采集、分析和流量测定。

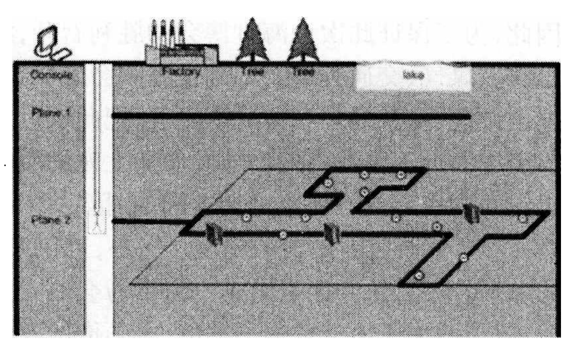
煤矿、石化、冶金行业对工作人员安全、易燃、易爆、有毒物质的监测的成本一直居高不下，无线传感器网络把部分操作人员从高危环境中解脱出来的同时，提高险情的反应精度和速度。

【应用实例 18.4】煤矿安全检测与定位系统

北京邮电大学的研究人员开展了煤矿瓦斯报警和矿工定位无线传感器网络系统的研究，系统结构如图 18.3 所示，一个节点上包括了温湿度传感器、瓦斯传感器、粉尘传感器等。传感器网络经防爆处理和技术优化后，可用于危险工作环境，在煤矿工作的员工及其周围环境将可以得到随时监控。



(a)



(b)

图 18.3　无线传感器网络用于煤矿监测

(a)煤矿安全检测与定位系统；(b)煤矿安全检测与定位系统。

18.3.2　先进制造

随着制造业技术的发展，各类生产设备越来越复杂精密。现在工作人员从生产流水线到复杂机器设备，都尝试着安装相应的传感器节点，以便时刻掌握设备的工作健康状况，及早发现问题及早处理，从而有效地减少损失，降低事故发生率。

【应用实例 18.5】电子科技大学、中国空气动力研究与发展中心以及北京航天指挥控制中心的研究人员，利用无线传感器网络进行大型风洞测控环境的监测，对旋转机构、气源系统、风洞运行系统，以及其他没有基础设施而有线传感器系统安装又不方便或不安全的应用环境进行全方位检测[1]。

18.3.3　交通控制管理

【应用实例 18.6】美国国家智能交通系统

1995 年美国交通部提出了“国家职能交通系统项目规划”，预计到 1825 年全面投入使用。该系统综合运用大量传感器网络，配合 GPS 系统、区域网络系统等资源，目的是使所有车辆都能保持在高效、低耗的最佳运行状态，前后自动保持车距，推荐最佳路线，并就潜在的故障发出警告。目前，美国的宾夕法尼亚州的匹兹堡市就已经建有这样的交通信

息系统,并由电台媒体附带产生了一定的商业价值[1,2]。

18.3.4　安防系统

【应用实例 18.7】英国的一家博物馆利用无线传感器网络设计了一个报警系统,将节点放在珍贵文物或艺术品的底部或背面,通过侦测灯光的亮度是否改变,测量物品是否遭受到振动等因素,来确保展览品的安全[1]。

18.3.5　仓储物流管理

利用无线传感器网络的多传感器高度集成,以及部署方便、组网灵活的特点,可用来进行粮食、蔬菜、水果、蛋肉存储仓库的温度、湿度控制,中央空调系统的监测与控制,厂房环境控制以及特殊实验室环境的控制等,为保障存货质量安全、降低能耗提供解决方案,如图 18.4 所示。

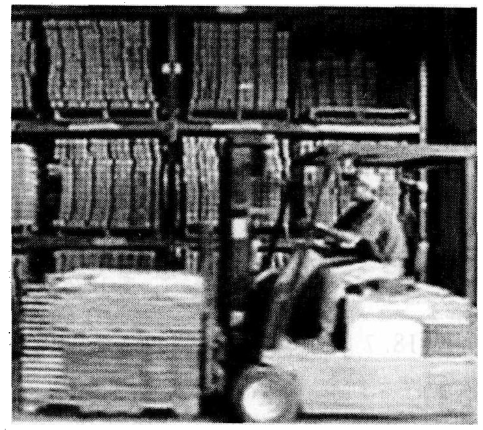



图 18.4　物流管理

【应用实例 18.8】超市中应用无线传感器网络进行各种物流和环境监测

著名的沃尔玛连锁店已经投入资金,在其货物上加装无线传感器节点和射频识别条型码芯片(RFID),以保证其各类货物处在最佳的储藏环境,同时,使该公司和供应商能够跟踪从生产到收款台的商品流向,如图 18.5 所示。



图 18.5　超市中应用无线传感器网络进行各种物流检测和环境监测

18.4　农业领域

我国是农业大国，农作物的优质高产对一个国家的经济发展意义重大。在这些方面，无线传感器网络有着卓越的技术优势。它可用于监视农作物灌溉情况、土壤空气变更、牲畜和家禽的环境状况以及大面积的地表检测。在国外，无线传感器网络已经应用到数字农业系统当中，如图 18.6 所示[1,3,4,15]。

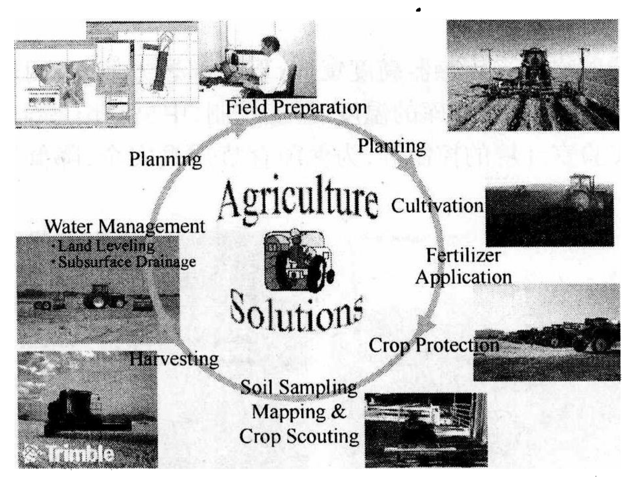


图 18.6　数字农业示意图

如图 18.7 所示，一个典型的系统通常由环境监测节点、基站、通信系统、互联网以及监控软硬件系统构成。根据需要，人们可以在待测区域安放不同功能的传感器并组成网络，长期大面积地监测微小的气候变化，包括温度、湿度、风力、大气、降雨量，收集有关土地的湿度、氮浓缩量和土壤 pH 值等，从而进行科学预测，帮助农民抗灾、减灾，科学种植，获得较高的农作物产量。在“九五”计划中，“工厂高效农业工程”已经把智能传感器和传感器网络化的研制列为国家重点项目。以下介绍几种国内外在这个领域所做的一些尝试。

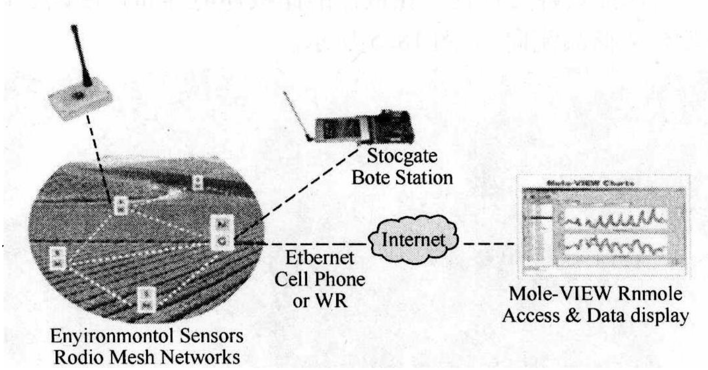


图 18.7　农业生态环境监测实例结构图

【应用实例 18.9】葡萄园环境监测系统应用方案

2002 年，英特尔公司率先在俄勒冈建立了世界上第一个无线葡萄园。传感器节点被

分布在葡萄园的每个角落，每隔一分钟检测一次土壤温度、湿度或该区域有害物的数量，以确保葡萄可以健康生长。研究人员发现，葡萄园气候的细微变化可极大地影响葡萄酒的质量。通过长年的数据记录以及相关分析，便能精确的掌握葡萄酒的质地与葡萄生长过程中的日照、温度、湿度的确切关系。这是一个典型的精准农业、智能耕种的实例，如图 18.8 所示。

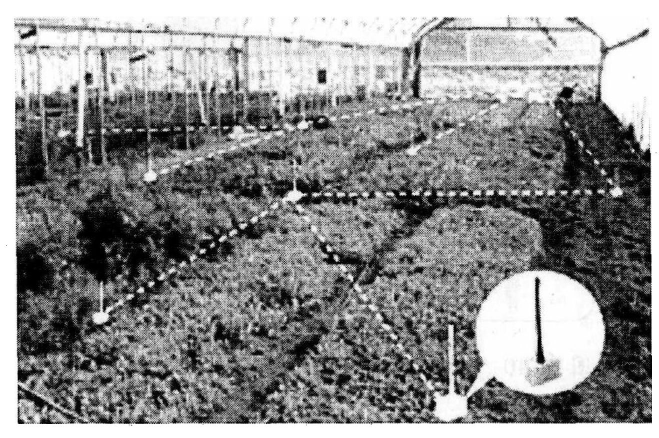


图 18.8　葡萄园环境监测系统示意图

【应用实例 18.10】温室环境应用方案

北京市科委计划项目“蔬菜生产智能网络传感器体系研究与应用”正式把农用无线传感器网络示范应用于温室蔬菜生产中。在温室环境里单个温室即可成为无线传感器网络的一个测量控制区，采用不同的传感器节点构成无线网络来测量土壤湿度、土壤成分、pH 值、降水量、温度、空气湿度和气压、光照强度、CO_2 浓度等，来获得农作物生长的最佳条件，为温室精准调控提供科学依据。最终使温室中传感器、执行机构标准化、数字化、网络化，从而达到增加作物产量、提高经济效益的目的，如图 18.9 所示。

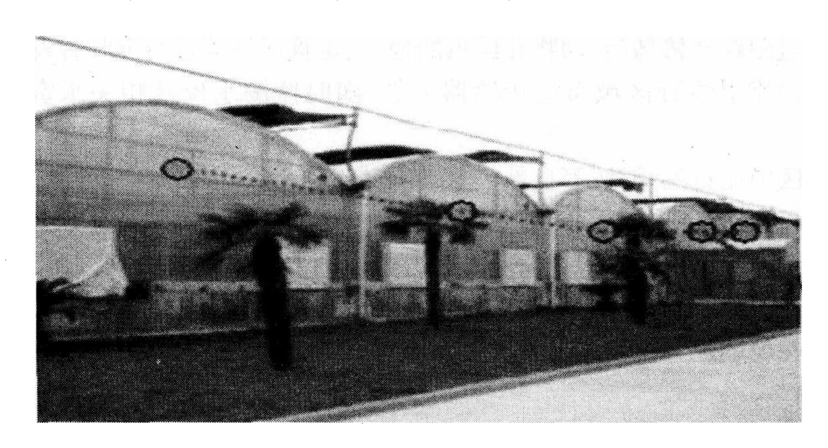


图 18.9　多温室间无线传感器网络通信的示意图

【应用实例 18.11】Digital Sun 公司自动洒水系统应用方案

Digital Sun 公司发展的自动洒水系统 S. Sense Wireless Sensor 是一套自动化无线传感器网络系统，该系统能够在没有工作人员管理与控制的情形下，有效且全自动地管理家庭花园内洒水的工作。该系统方案很好地解决了人工洒水不适用场合的洒水问题。

该自动洒水系统应用方案的系统示意图如图18.10所示。它使用无线传感器感应土壤的水分，并在必要时与接收器通信，控制灌溉系统的阀门打开/关闭，从而达到自动、节水灌溉的目的。

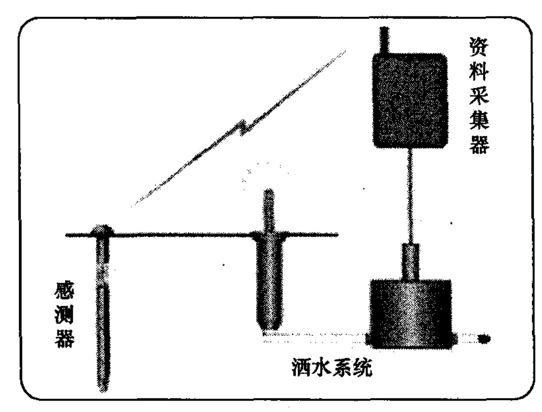


图18.10　Digital Sun公司自动洒水系统示意图

该方案不仅具有完成自动洒水工作的能力，同时也具有检测系统是否出了相关问题的能力，以便让管理者来进行维修等工作。该方案很有创意性，表现出了很好的人性化和智能化，虽然该方案相对比较简单，但是有很强的实用性。

18.5　其他领域的典型应用

18.5.1　环保监测

无线传感器网络可以广泛地应用于生态环境监测、生物种群研究、气象和地理研究、洪水、火灾检测。以下列出了一些常见的应用领域：

(1)可通过跟踪珍稀鸟类、动物和昆虫的栖息、觅食习惯等进行濒临种群的研究等。

(2)可在河流沿线分区域布设传感器节点，随时监测水位及相关水资源被污染的信息。

(3)在山区中泥石流、滑坡等自然灾害容易发生的地方布设节点，可提前发出预警，以便做好准备，采取相应措施，防止进一步的恶性事故的发生。

(4)可在重点保护林区铺设大量节点随时监控内部火险情况，一旦有危险，可立刻发出警报，并给出具体方位及当前火势大小，如图18.11所示。

(5)布放在地震、水灾、强热带风暴灾害地区、边远或偏僻野外地区，用于紧急和临时场合应急通信[1]。

【应用实例18.12】大鸭岛生物环境监测系统应用方案

2002年，由英特尔的研究小组和加州大学伯克利分校以及巴港大西洋大学的科学家把无线传感器网络技术应用于监视大鸭岛海鸟的栖息情况，如图18.12所示。位于缅因州海岸大鸭岛上的海燕由于环境恶劣，海燕又十分机警，研究人员无法采用通常方法进行跟踪观察。为此他们使用了包括光、湿度、气压计、红外传感器、摄像头在内的近10种传感器类型数百个节点，系统通过自组织无线网络，将数据传输到300英尺外的基站计算机

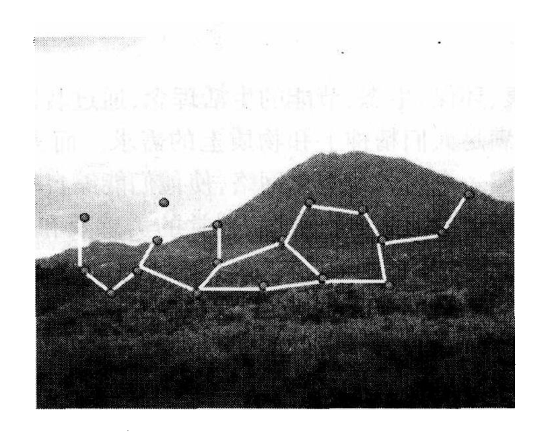


图 18.11　森林防火监测

内，再由此经卫星传输至加州的服务器。在那之后，全球的研究人员都可以通过互联网察看该地区各个节点的数据，掌握第一手的环境资料，为生态环境研究者提供了一个极为有效便利的平台。

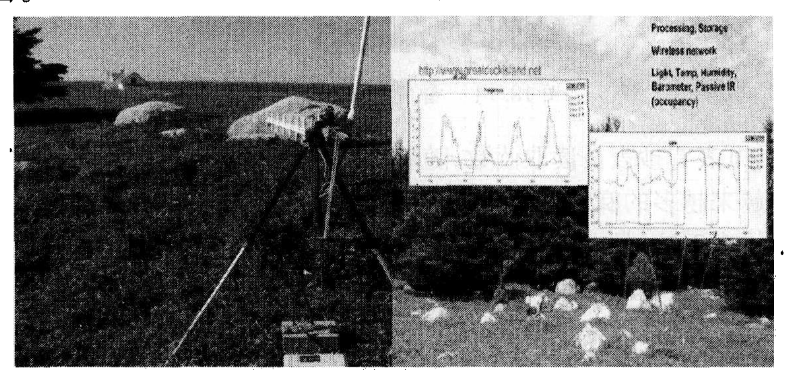


图 18.12　大鸭岛生态环境监测系统示意图

【应用实例 18.13】北澳大利亚蟾蜍的分布情况监测应用方案

2005 年，澳洲的科学家利用无线传感器网络来探测北澳大利亚蟾蜍的分布情况，如图 18.13 所示。由于蟾蜍的叫声响亮而独特，因此，利用声音作为检测特征非常有效。科研人员将采集到的信号在节点上就地处理，然后将处理后的少量结果数据发回给控制中心。通过处理，就可以大致了解蟾蜍的分布、栖息情况。

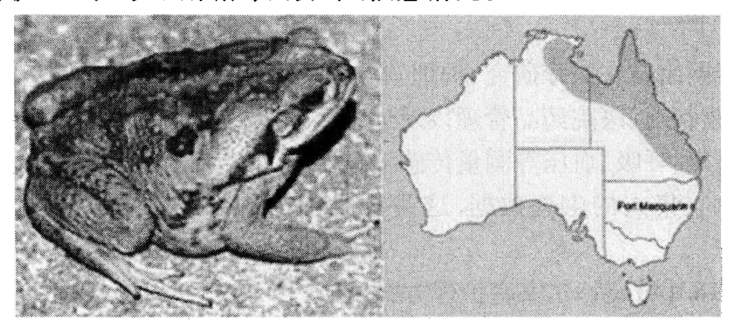


图 18.13　北澳大利亚的蟾蜍分布情况

18.5.2　智能家居

舒适家居是一种健康、环保、生态、节能的生活理念，通过装饰的美观性和居住的功能性两个方面来实现，分别满足人们精神上和物质上的需求。而无线传感器网络通过将各种家居设备联系起来，组建一个家居智能化网络，使他们能够自动运行，相互协作，实现居住的功能性，为居住者带来全面的家居安全感、视觉的美感及和谐感，提高了他们的生活品质，如图 18.14 所示[3,4]。

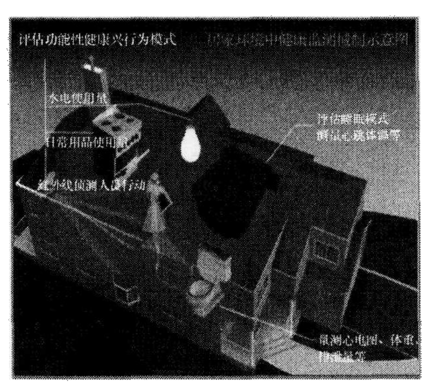


图 18.14　智能家居系统示意图

传统的水、电表有抄表员读取读数，随着社会的发展及高层建筑的普及、传统操作给抄表人员带来越来越多的麻烦。浙江大学计算机系的研究人员开发了一种基于无线传感器网络的无线水表系统，具有高度的自动化性能，抄表人员无需访问每户人家，只需在楼下按下抄表键，即可获得该楼的所有水表的读数。

复旦大学、电子科技大学等单位研制了基于无线传感器网络的智能楼宇系统。其典型结构包括照明控制、警报门禁、家电控制的 PC 机系统。各个部分可相互通信，最终由 PC 机通过互联网将信息发布在网络上，主人可以通过任何互联网终端检测家庭情况。该系统可对火患、盗窃等安全隐患进行检测报警，并能集中抄表。

电子樟脑丸是一种典型的智能家居产品，该设备实际上是具有温度和湿度传感器的无线传感器网络设备。它不能代替樟脑丸的防蛀、防霉作用，但是当它检测到衣橱中的温度湿度不合适衣物保存时，可通过手机短信或电话留言等方式，通知主人作适当处理。

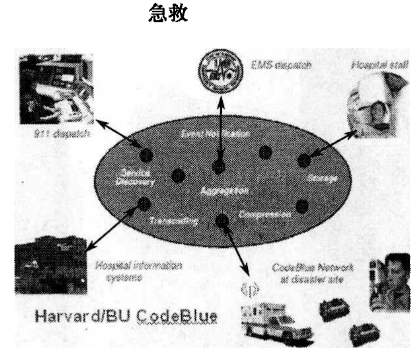
18.5.3　医疗监护

无线传感器网络在在医疗研究、护理领域表现出了它特有的优势，它在检测人体生理数据、老年人健康状况、医院药品管理以及远程医疗等方面可以发挥出色的作用。在病人身上安置体温采集、呼吸、血压等测量传感器，医生可以远程了解病人的情况。利用传感器网络长时间地收集人的生理数据，这些数据在研制新药品的过程中非常有用，如图 18.15 所示[1]。

【应用实例 18.14】英特尔家庭护理方案

该方案是英特尔为探讨应对老龄化社会的技术项目（Center for Aging Services Technologies，CAST）的一个环节而开发的，用于帮助老龄人士、阿尔茨海默氏病患者以及残障

急救



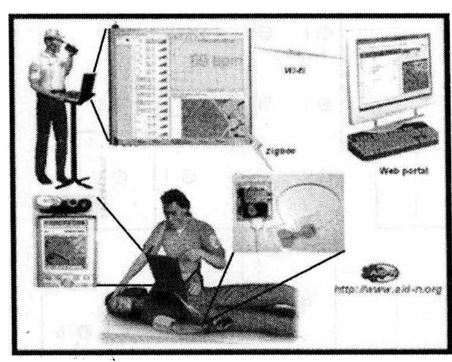


图 18.15　医疗监护示意图

人士的家庭生活。利用无线通信技术将各种传感器节点联网，可高效传递必要的信息从而方便护理。同时，通过该方案还可以减轻护理人员的压力负担。该方案是英特尔公司在护理阿尔茨海默氏病患者等家庭的合作下历时一年研究完成的。英特尔公司从 2004 年后半年已经开始在实际家庭中试运用该方案。

该方案通过在患者家中布置若干个传感器节点，由产感器节点采集患者所处环境的相关数据，而传感器节点之间以多跳路由的方式进行数据传递，然后将所采集到的数据都传送到一个通信、数据处理和存储能力相对较强的接收节点，最后该接收节点按一定周期时间把处理后的数据发送给医院的护理中心，再由护理中心对数据进行分析。即可知道患者的护理清况。

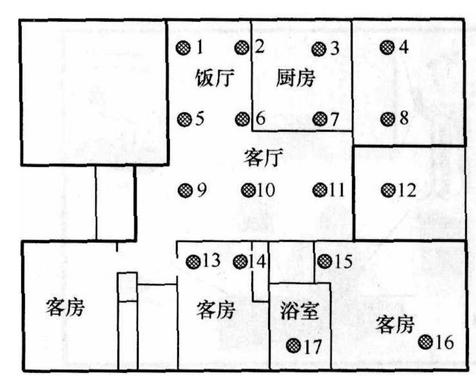
该方案的应用让患者在家里而不需要去医院就可以接收护理，同时系统能自动地把护理进展情况反映给医院。而医院更是可以通过这种发高科技技术，来实现不用见面就了解患者的情况。医疗中心通过了解到的情况对患者的护理方式进行及时的调整或者改变，这是医疗护理中工作方式的变革。

【应用实例 18.15】远程医疗监控系统应用方案

研究人员可以利用无线传感器网络来实现远程医疗监视。远程医疗监控系统如图 18.16 所示，在一个公寓内，17 个传感器节点分布在各个方间，包括卫生间。每个传感器节点上包括了温度、湿度、光、红外传感器及声音传感器，部分节点使用了超声节点。根据这些节点收集到信息，监控界面实时显示人员的活动情况。根据多传感器的信息融合，可以相当精确地判断出被检测人正在进行的行为，如做饭、睡觉、看电视、淋浴等，从而可以对老年人健康状况，如老年痴呆症等进行精确检测。因为系统不使用摄像机，比较容易得到病人及其家属的接受。

该方案中使用的是美国 Crossbow 公司所生产的有关无线传感器网络方面的器件，包括 17 个 MICAz、若干 Cricket、MTD310CA、Stargate、PC 机等。

该方案由基站和无线传感器节点构成一个无线传感器监护网络。传感器节点对所需要监测的、有关生命指标方面的数据进行采集，首先通过无线通信的方式将数据发送到基站，并由基站对数据进行较复杂的处理，如进行数据融合；然后通过因特网或者 GSM 网络将数据传输至远程医疗监控中心的服务器上，在远程医疗监控中心，专业医疗人员借助相关应用软件系统对数据进行处理分析，并显示报告结果；最后由专业医疗人员对报告进行



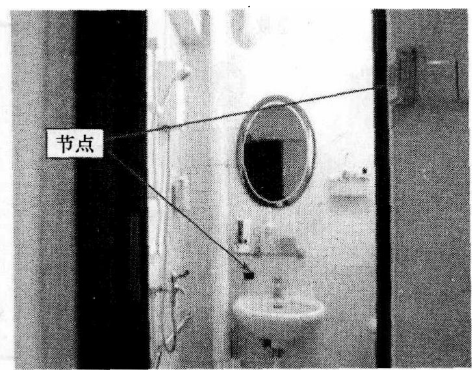


图 18.16　左图为公寓内无线传感器节点的分布图；右图为浴室中的节点分布图

分析，根据各自的情况提供必要的医疗方案和咨询服务等，实现远程医疗监护。

该方案是西安某科技有限公司开发的，在远程医疗上具有巨大的应用价值，目前该方案已经投入到实际应用。该方案能够看到无线传感器网络技术的优势，这本身就突破了技术问题，为以后中国的远程医疗方面的发展提供了良好的技术参考，将为中国的医疗现代化建设提供巨大的动力。

18.5.4　建筑领域

我国正处在基础设施建设的高峰期，各类大型工程的安全施工及监控是建筑设计单位长期关注的问题，如已经建成的三峡工程，正在建设的苏通大桥、渤海海域的大量的海洋平台和海底管线、2008 年的奥运场馆等。采用无线传感器网络，可以让大楼、桥梁和其他建筑物能够自身感觉并意识到它们的状况，使得安装了传感器网络的智能建筑自动告诉管理部门它们的状态信息，从而可以让管理部门按照优先级进行定期的维修工作[1,3]。

【应用实例 18.16】基于无线传感器网络的桥梁安全监测系统应用方案

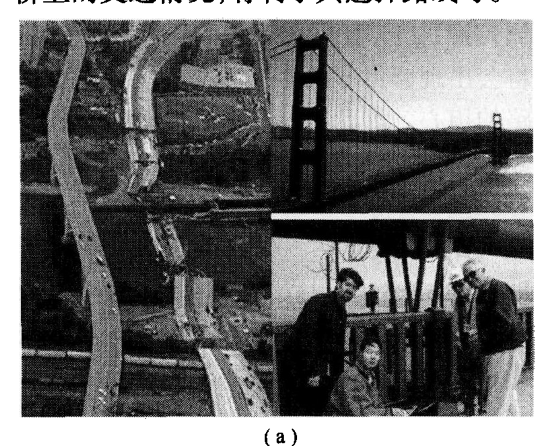
在国内外，经常发生桥梁断裂坍塌的事故，这些事故的发生，引起了人们对桥梁结构等建筑结构的安全性的重视，桥梁安全监测系统就应运而生了。

利用适当的传感器，如压电传感器、加速度传感器、超声传感器、湿度传感器等，可以有效地构建一个三维立体的防护检测网络。该系统可用于监测桥梁、高架桥、高速公路等道路环境。对许多老旧的桥梁，桥墩长期受到水流的冲刷，传感器能够放置在桥墩底部、用以感测桥墩结构；也可放置在桥梁两侧或底部，搜集桥梁的温度、湿度、震动幅度、桥墩被侵蚀程度等，能减少断桥所造成生命财产的损失。

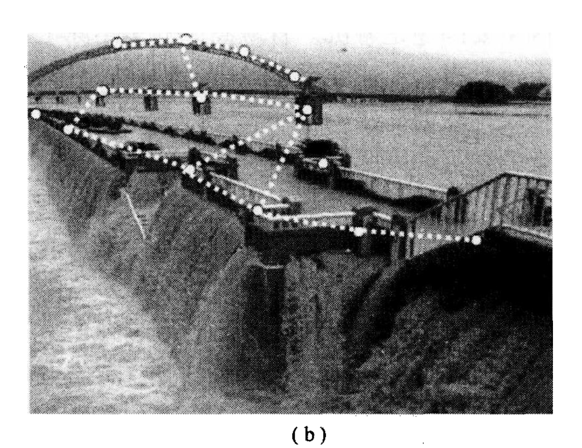
如图 18.17 所示的方案中，首先传感器节点通过无线通信技术把数据发送到每个桥梁监测处的数据接收点（Sink 节点或汇聚节点）。再由数据接收点对各类数据进行较复杂的处理和存储，然后借助卫星通信网络或者以太网等网络把数据发送到信息中心，信息中心的软件系统对数据进行分析处理并发送到相关的管理部门的网站中去，最后管理部门根据信息中心传送来的数据分析结果来了解和掌握桥梁的情况，同时还可以根据分析结果，通知相关部门来展开对桥梁的维护工作。

该系统作为监测通信平台，其覆盖的范围不单单只是在桥上和桥梁附近，同时也包括了陆地，当监测到桥上发生突发事故等，严重影响到交通的进行时，可以与交管、公安警察

等部门进行通信,共同指挥、协同完成事故的处理。该方案在进行对桥梁的监测的同时,也可以为需要通过该桥的行驶用户提供相关信息的网络接入,这样用户可以很好地了解桥上的交通情况,有利于其选择路线等。



(a)



(b)

图 18.17　无线传感网络用于桥梁和大坝监测

(a)基于无线传感器网络的桥梁安全监测系统;(b)基于无线传感器网络的大坝安全监测系统。

【**应用实例 18.17**】无线传感器网络应用于珍贵文物的保护系统应用方案

对珍贵的古老建筑进行保护,是文物保护单位长期以来的一个工作重点。将具有温度、湿度、压力、加速度、光照等传感器的节点布放在重点保护对象当中,无需拉线钻孔,便可有效地对建筑物进行长期的监测。此外,对于珍贵文物而言,在保存地点的墙角、天花板等位置,监测环境的温度、湿度是否超过安全值,可以更妥善地保护展览品的品质,如图 18.18 所示。

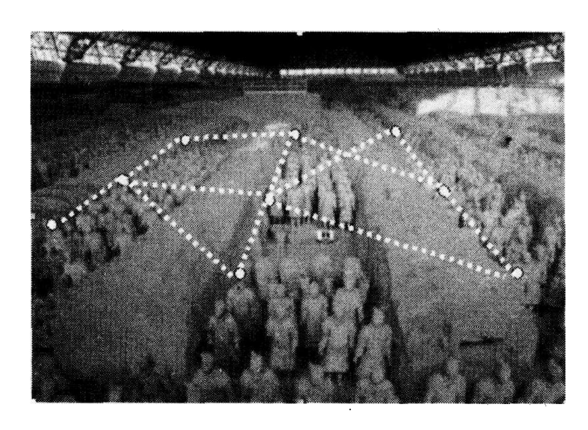


图 18.18　将无线传感器网络应用在珍贵文物的保护场地

【**应用实例 18.18**】青藏铁路冻土试验路基内部应变智能监测系统应用方案

在我国东北和西北有一百多万平方千米的多年冻土,南部边缘的冻土厚度较薄,区内大部分冻土是属于不稳定的。究其原因,除气候条件严寒之外,主要是对边缘冻土的特性缺乏认识,因此这些地区铁路的修建工作一直是在边修建、边冻害、边摸索的情况下进行的。许多工程冻害不仅在铁路运营之前就很严重,在交付运营之后,时隔几年或十几年仍在陆续出现新的冻害,其冻害程度在我国铁路史上也是罕见的,引起路内外工程界人士的

关注。青藏铁路长 1118km，其中，多年冻土区长度为 632km，大片连续多年冻土区长度约 550km，岛状不连续多年冻土区长度 82km，全线海拔 4000m 以上地段长度约为 965km。冻土区筑路遇到的主要问题是冻胀和融沉。在季节冻土区主要问题是冻胀，在多年冻土区主要问题是融沉。青藏高原的多年冻土大多属高温冻土、极易受工程的影响产生融化下沉。有的专家看后曾预言，青藏铁路修建后，将会出现修得起而养不起的被动局面。这种议论在前些年确实代表了许多人对冻土区修路的担心。因此，认识和研究冻土，掌握冻土的融沉和冻胀特性，是减轻高寒地区铁路、公路冻害的必由之路，监测冻土位移随温度变化的规律是研究冻土融沉和冻胀特性主要内容。

该系统通过在青藏高原多年冻土地区铺设试验路段，能长期测量路基及路基下面冻土层的温度和应变以及季节活动层沿路基走向的变形，并把监测数据从青藏试验路基现场自动传输到千里之外的研究人员办公室的电脑中。监测的目的在于通过对监测数据进行分析，了解冻土冻胀和融沉的规律，为青藏铁路和公路地基设计提供数据和理论依据。

【应用实例 18.19】建筑物风险监测系统应用方案

在建筑物的使用过程中可能要遭受自然灾害和人为事件的影响，如地震、台风、火灾等。为了很好地对这些灾难和人为事件进行预防，减少其带来的经济损失及人员伤亡，通过利用无线传感器网来对建筑物结构的一些物理量的数据采集和建筑物环境的数据采集，再由建筑物风险监测系统的软件系统对收集到的数据进行分析，从而可以对一些灾难和人为事件进行发现和预测，让整个建筑物处于和谐的环境中。

在该方案中由于要采集的数据种类比较多，因而用到的传感器节点的种类和数目很多。该方案中，既要对建筑物的结构进行监测，又要对建筑物中的一些突发事件进行发现，如某个房间里漏气、火灾、自杀事件等，还要对建筑物中的温度等进行监测。该方案的无线传感器网络是网状网络，传感器节点之间通过多跳方式对数据进行传递，而且在每个建筑物处建立一个基站，基站接受来自所有传感器节点的数据并对其进行数据融合，经过处理后发送到监测中心，监测中心利用相关专家系统等应用软件对数据进行分析并得出结果。

当系统发现了建筑物中有突发事件发生时（如当发生火灾时），监测中心可以立即发布信息，对建筑物中的人进行安全的疏散；当发现有人自杀等时，监测中心可以通过与公安等部门联系来避免事故的发生。通过对建筑物结构的监测，可以对建筑物进行相关的维护，当有台风等自然灾害发生时，可以根据建筑物的结构承受能力来发布相当的信息。例如，在台风发生时，由于高建筑物会有所摆动，根据程度公告建筑物中的办公人员和居民等注意安全防范，不要在建筑物内进行可能影响到建筑物安全的活动。

该方案中的应用软件系统包括很多子系统，其不仅完成对建筑物的结构安全进行监测，可以及时地发现建筑物结构中可能存在的安全隐患，还可以对一些火灾、漏气等事故进行发现，这样大大降低了因这些事故可能带来的巨大的经济损失和对生命安全的威胁。对于一些大型的复杂建筑物该方案更能体现出其价值所在，故该方案已经得到很好的推广应用。

18.5.5　自然灾害预警

每年在国内许多地区都遭受不同的自然灾害的威胁，无线传感器网络可以适用于山

洪、泥石流等自然灾害的多发区，很好地对自然灾害进行预测等，如图 18.19 所示[1]。

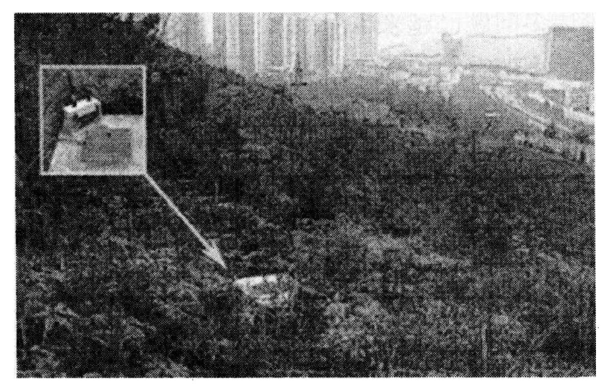


图 18.19　山体滑坡监测

【应用实例 18.20】安第斯山脉地区山洪预警系统应用方案

近年来根据报道得知，在委内瑞拉德安第斯山脉地区的城市 Merida 及其附近城镇因山洪而带来了巨大财产损失和人员伤亡。另外，根据从水利和地理方面的研究显示，未来该地区还是一个很容易爆发山洪的地方。为此专家们根据安第斯山脉的地质结构等设计开发了安第斯山脉地区山洪预警系统应用方案。从空间方面看，该方案横跨由布置无线传感器网络的监测区（山区）和具有预警指挥控制功能的城区两个区域。在无线传感器网络中，由用来监测水文、气象和山脉活动情况 3 类传感器节点来构成。监测水文方面的节点沿着河流两岸进行布置，用来采集河流水位和水流方面的数据；监测气象方面的节点放置在河流的附近地区，用来采集和感知光线、温度、湿度、大气气压、风向和风速等数据；监测山脉活动情况的节点布置在山脉的一些特定区域，用来监测地震波、土壤湿度和移动情况。这些传感器节点由于要处理比较多的数据，从而采用太阳能技术。传感器节点通过汇聚节点把数据发送到城区的预警指挥中心，预警指挥中心根据相关专家系统和 GIS 系统对数据进行分析，对警告信号进行分级和对可能发生灾难的地区位置通过 GIS 的数字地图显示出来，同时预警中心可以把这些相关分析的结果放到因特网供用户浏览。预警系统就根据分析的结果，通过在电视、广播电台中发布预警信息，包括可能发生灾害的位置和严重程度等。在所收集到的数据可以存储到系统中，以便将来进行参考使用。

该方案可以预先知道可能发生的灾害，为预防灾难做很好的准备，大大减少了因灾害所带来的人员伤亡和经济损失。

18.5.6　目标跟踪应用

在无线传感器网络的许多应用中，跟踪运动目标是一项基本功能。目标跟踪需要传感器网络根据节点的侦测信号判断目标是否出现。如果目标出现，需要在一定时间内判断出目标的运动轨迹。这就不仅要求传感器节点对侦测数据进行处理，根据不同的任务需求和有限资源选择合适的算法确定目标状态，而且需要网络中的多个节点协同工作，通过交换侦测信息共同确定目标的运动轨迹，并将跟踪结果发送给网络用户[1]。

【应用实例 18.21】高速公路交通监控系统应用方案

随着经济的高速发展，要求对经济建设所需的物质在运输中所花的时间越短越好。

因此，高速公路也相应地得到迅速发展。在高速公路中。如何来提高交通效率、保障交通安全、加强交通管理等诸多问题已越来越受到重视。这些问题促使高速公路不断向着信息化、网络化和智能化的方向发展。在这些方面高速公路交通监控系统发挥了重要的作用，现有的高速公路交通监控系统绝大部分都是采用图像处理技术、雷达波检测技术、电磁感应技术等，但由于这些技术自身存在延迟大、距离、可靠性低、受环境限制明显等局限性，均无法全面、实时、有效地实现高速公路的交通监控。基于无线传感器网络技术的高速公路交通监控，充分利用无线传感器网络的分布性、灵活性、动态性及无线通信等特点，将有效改善现有交通监控系统的功能。

系统框架如图 18.20 所示。与现有交通监控系统相同，本方案采用分层管理的三层结构来构建此系统。无线传感器网络作为监控子系统的重要组成部分，来实现严重汽车追尾的预防、能见度低等情况下的信息采集等功能，构建一个功能更加完善、效果更高的高速公路交通监控系统。

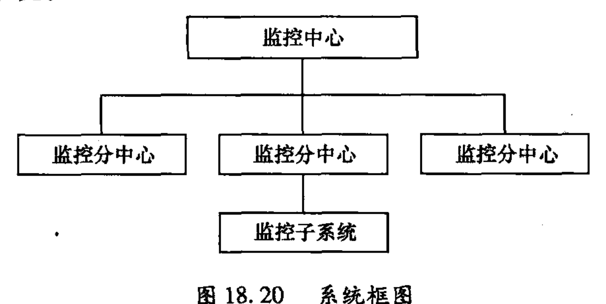


图 18.20　系统框图

由图 18.20 可知，高速公路交通监控系统主要由监控中心、若干监控分中心和监控子系统来组成，在这些组成部分中，它们都具有不同的专门的功能，来负责完成不同的工作。

(1) 监控中心。负责接收各分中心监控系统传输的各种数字和图像信息，监控所管辖的高速公路的交通运行状况，并向各监控分中心发布各种控制命令。

(2) 监控分中心。负责各自高速公路管辖区段的外场设备、采集各种数字和图像信息、接收和发布各种控制命令、以及传输各种数字和图像信息。

(3) 监控子系统。由各种外场设备自身所形成的相对独立的子系统，主要用于监控车流、路况、能见度及气象状况等。

无线传感器网络是该系统的重要组成部分之一。该系统的无线传感器网络和其他系统的无线传感器网络一样，主要可分为以下 3 层。

(1) 传感器节点。收集和感知监控区域中行驶车辆的相对速度、车距等参数。传感器节点采集信息后，由传感器本身的处理器对信息进行初步处理，并通过通信接口将处理过的信息发送给基站，基站对所属区域内所有节点传递的信息进行融合处理后，获得进一步的测量数据的结果。最后，系统内所有基站的数据将传送给系统的处理中心。

(2) 基站。比传感器节点具有更多能源和更大处理能力，它对本区域内所有传感器节点所采集和初步处理后的信息进行融合处理，提炼出监控系统所需要的数据。

(3) 处理中心。位于监控系统的最上层，处理中心是整个系统的中心和决策机构，它具有相应的数据库系统，并具有控制决策功能。负责处理、分析下层传来的信息，对监控路段内的所有车辆的运行状况及时了解，并进行决策。

高速公路交通监控系统具有及时准确地采集车辆、路况及主要交通设施的状态信息等的功能；对高速公路实现全程、实时跟踪监控；根据监控系统所获取的信息，迅速采取相应处理和优化控制方案，并立即执行；建立多种信息发布渠道，为用户提供有用信息；对交通事故做出快速响应，迅速排除事故根源和提供救援服务等。将无线传感器网络与传统技术结合所构建的新型高速公路交通控制系统，更加完善现有高速公路交通监控系统的功能。系统的投入应用将为中国高速公路信息化建设发挥巨大作用。

18.5.7　空间和海洋应用

无线传感器网络有着十分广泛的应用前景，它不仅在军事、安全、工业、农业、环境监测、智能家居、医疗监护、土木建筑等传统领域具有巨大的应用价值，未来还将在许多新兴领域体现其优越性，如空间探索、海洋探索等领域。可以大胆地预见，将来无线传感器网络将无处不在，其应用可以涉及到人类日常生活和社会生产活动的所有领域，将完全融入人们的生活。

1. 空间探索方面

探索外部星球一直是人类梦寐以求的理想，借助于火箭、太空舱或探路者布撒的传感器节点实现对星球表面大范围、长时期、近距离的监测和探索，为人类登陆做准备，这是一种经济可行的方案。NASA 的 JPL 实验室研制的 Sensor Webs 就是为将来的火星探测、选定着陆场地等需求进行技术准备的。现在该项目已在佛罗里达宇航中心的环境监测项目中进行测试和完善，如图 18.21 所示。

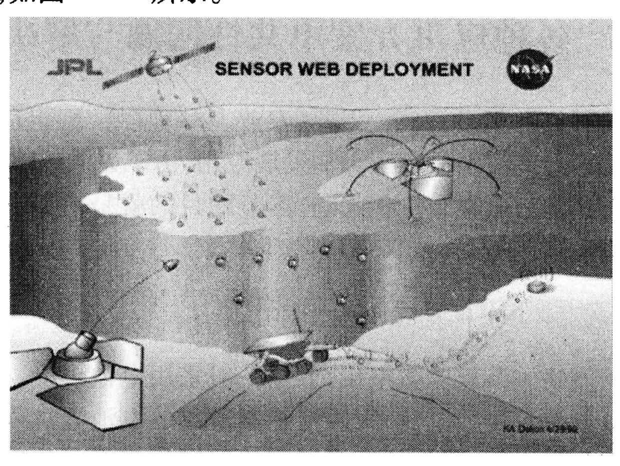


图 18.21　美国宇航局的空间探索计划中无线传感器网络的应用模式示意图

最近，我国国家自然科学基金重点项目“月球探测系统的建模、传感、导航和控制基础理论及关键技术研究”在合肥召开了项目进展汇报与研讨会。会中指出：在月球探测车月面导航技术方面，在传统的陀螺、视觉和激光导航的基础上，提出了基于无线传感器网络的月球探测车传感、导航、定位方法，为月球探测车消除定位和导航的积累误差以及动态构建月面环境地图与自主路标设置提供了新的方法。这些研究成果对提高我国月球探测系统的技术水平和加强技术储备，实现探月工程的“落、返”目标具有重要意义。

2. 海洋探索方面

18 世纪是人类深入开发利用海洋资源的世纪，海洋物理研究、数据采集、交通导航、

资源勘探、污染监控、灾难预防，以及对水下军事目标的监测、定位、跟踪与分类等，都迫切需要高度智能化、自主性强、分布式、全天候的信息采集、传输、处理及融合技术。印度洋海啸之后，全球领导人在印尼雅加达举行峰会，议程的首要事务就是计划在印度洋构建传感器网络，以便对未来的海底地震做出预警。

针对这些要求，基于多传感器的水下分布式信息采集、网络通信、信息处理技术得到国家广泛关注，并随着近些年通信技术、DSP 技术、MEMS 传感器技术等相关领域的迅猛发展，成为我国国民经济及军事国防领域一项亟待研究开发的重要课题，如图 18.22 和图 18.23 所示。

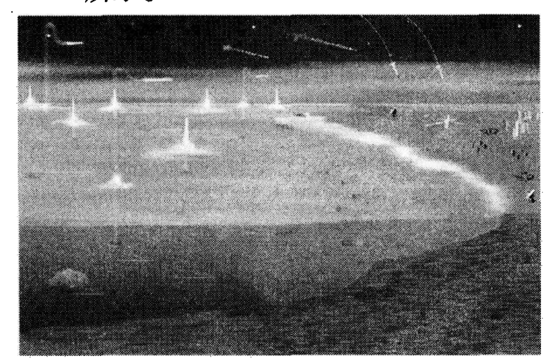


图 18.22　水下无线传感器网络技术示意图

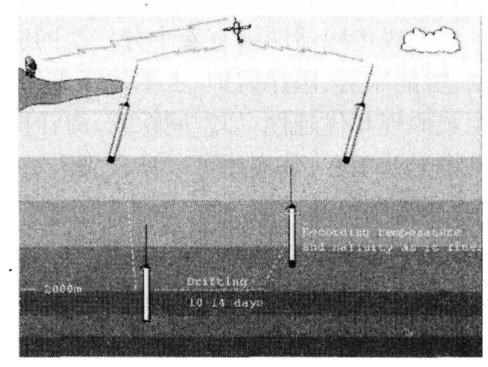


图 18.23　深海监控示意图

18.6　各种应用方案中共性问题与解决思路

虽然无线传感器网络在军事、安全、工业、农业、环境监测、智能家居、医疗监护、土木建筑等领域的用途都已经或将要得到很大的发展应用，由于无线传感器网络自身的缺点，这些应用方案不可避免地将会存在一些问题，本节的目的就是指出上述方案中普遍存在的问题及其解决的方案。

18.6.1　无线传感器网络中节点的能量问题

由于无线传感器网络中节点的微型化，节点一般采用电池供电，电池的能量有限，而且由于物理限制难以给节点更换电池，所以传感器节点的电池能量限制是整个无线传感器网络设计最关键的约束之一，它直接决定了网络的工作寿命。传感器节点消耗能量的模块包括传感器模块、处理模块和无线通信模块，其中绝大部分的能量消耗在无线通信模块上，通常 1bit 信息传输 100m 距离所需的能量大约相当于执行 3000 条计算指令所消耗的能量。

降低能耗是无线传感器网络软、硬件设计的重点。主要的解决方法是在节点设计中采用低功耗硬件、电源管理、功率管理、设计节能且简单高效的 MAC 和路由协议、减少通信数据转发和有效的拓扑管理等。

18.6.2　传感器节点的时钟同步要求

时间同步是无线传感器网络应用的重要组成部分，传感器数据融合、传感器节点自身

定位等都要求节点间的时钟保持同步。虽然不同的应用场合对无线传感器网络时钟同步的要求会有所不同,但就整体来说,无线传感器网络的时间同步主要面临下面几个问题:

(1)通常无线传感器网络节点数目多、部署密集,节点之间时间同步信息在关键路径上的传输延迟具有很大的不确定性。

(2)由于节点的移动、能量耗尽以及和周围环境的影响等原因,无线传感器网络的拓扑结构变化频繁,从而难以预先确定获取基准时间的关键路径。

(3)为了降低节点的能量消耗,往往会设计一些协议使得节点大部分时间处于休眠状态,而这些休眠的节点不能持续保持时间同步。

(4)对于大规模传感器网络,基准时间的传递将是要重点解决的问题,也因此引出整个网络的全局时间同步精度难以确定的问题。

(5)目前,能量消耗仍然是在设计时间同步机制时需要考虑的因素。

在实际中时钟同步有两种模型,一种是相对时钟同步,即每一个节点存储各自的本地时钟和与子网中任意其他节点的时钟之间的相对偏移信息;另一种是"always on"模型,即每个节点都保持一个时钟,每个时钟与网络中的一个参考节点通过"发送者—接收者握手"实现绝对时钟同步。

18.6.3　各方案中共性问题解决思路

针对各方案中的共性问题,提供以下解决思路:

(1)无线传感器网络的通信速率较低,真正的数据发送量很少。解决这个问题的办法可以让无线传感器网络中的中间节点尽量多做些数据处理工作,尽量减少原始数据的发送量。例如,在危险工作环境的监控中,对于平稳状态的原始数据可以不发送到数据中心,只发送出超出允许状态前后的原始数据,这样能大大减少数据的通信量,同时也降低了整个网络的能耗。

(2)无线传感器网络的拓扑结构的确定。无线传感器网络的拓扑结构可以结合故障传播路径确定。利用相关的统计过程监测算法可以区分不可识别扰动或故障,从而将无线传感器网络故障分辨率方面的设计困难转移到后续的监测算法上去。

(3)对无线传感器网络的维护和管理工作。这个问题可以通过定期检查并更换无线传感器网络中的失效节点,测试网络性能等来解决。

参考文献

[1] 韩红彦,张西红,王卫国,张晓. WSN的关键问题及军事应用[J]. 科学技术与工程,2007,7(7)1465-1467.

[2] 叶湘滨,陈利虎,胡罡. 无线传感器网络在环境监测中的应用[J]. 计算机测量与控制,2004,12(11)1033-1035.

[3] 杨唐胜. 青藏铁路冻土试验路基内部应变智能监测系统研究[D]. 武汉:武汉大学,2005.

[4] http://www.wsns.net.cn.